GUÍA DE IMPLEMENTACIÓN

CÓMPUTO DEL USUARIO FINAL DE EMC VSPEX

VMware Horizon View 6.0 y VMware vSphere con EMC XtremIO

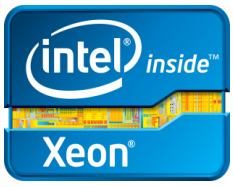
Con tecnología de EMC Isilon, EMC VNX y EMC Data Protection

EMC VSPEX

Resumen

En esta guía de implementación se describen los pasos generales requeridos para implementar una solución de cómputo del usuario final de EMC® VSPEX® para VMware Horizon View y VMware vSphere con EMC XtremIO™ y con tecnología de EMC Isilon®, EMC VNX® y EMC Data Protection.

Marzo de 2015



EMC²

Copyright © 2014 EMC Corporation. Todos los derechos reservados. Publicado en México.

Publicado en marzo de 2015

EMC considera que la información de este documento es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

La información de esta publicación se proporciona tal cual. EMC Corporation no se hace responsable ni ofrece garantía de ningún tipo con respecto a la información de esta publicación y específicamente renuncia a toda garantía implícita de comerciabilidad o capacidad para un propósito determinado. El uso, la copia y la distribución de cualquier software de EMC descrito en esta publicación requieren una licencia de software correspondiente.

EMC², EMC y el logotipo de EMC son marcas registradas o marcas comerciales de EMC Corporation en los Estados Unidos y en otros países. Todas las demás marcas comerciales utilizadas en este documento pertenecen a sus respectivos propietarios.

Para obtener una lista actualizada de nombres de productos de EMC, consulte las marcas comerciales de EMC Corporation en mexico.emc.com (visite el sitio web de su país correspondiente).

Cómputo del usuario final de EMC VSPEX
VMware Horizon View 6.0 y VMware vSphere con EMC XtremIO
Con tecnología de EMC Isilon, EMC VNX y EMC Data Protection
Guía de implementación

Número de referencia H13313.1

Contenido

Capítulo 1 Introducción 9
Propósito de esta guía 10
Valor para el negocio 10
Alcance 11
Audiencia 11
Terminología 12

Capítulo 2 Antes de comenzar 13
Descripción general 14
Tareas previas a la implementación 14
Flujo de trabajo de implementación 15
Lectura esencial 15
Descripción general de la solución VSPEX 15
Guía de diseño de VSPEX 15
Guía de la infraestructura comprobada VSPEX 16
Guía de respaldo y recuperación de EMC para VSPEX 16
Prerrequisitos de la implementación 16

Capítulo 3 descripción general de la solución 19
Descripción general 20
Infraestructuras comprobadas VSPEX 20
Arquitectura de la solución 21
Arquitectura de alto nivel 21
Arquitectura lógica 23
Resumen de los componentes clave 24

Capítulo 4 Implementación de la solución 25
Descripción general 26
Implementación de la infraestructura de red 27
Configurar la red de la infraestructura 27
Configuración de las VLAN 28
Configurar la red de almacenamiento 29
Conectar el cableado de la red 29
Preparación y configuración de los arreglos de almacenamiento 30
Preparar el arreglo XtremIO 31
Preparar el cluster de Isilon 31
Preparar el arreglo VNX 31
Configurar el arreglo XtremIO inicial 31
Configurar el cluster de Isilon inicial 32

Configurar del arreglo VNX inicial 32
Provisionar almacenamiento para áreas de almacenamiento de datos de VMFS .. 32
Configurar VNX FAST Cache 33
Provisionar almacenamiento opcional para los datos de usuario 34
Configurar FAST VP para los datos de usuario en VNX (opcional) 36
Requisitos de la nube privada de VSPEX 38
Configurar controladores de eventos de XtremIO 38
Instalación y configuración de los hosts vSphere 40
Instalar vSphere 41
Configurar la red vSphere 41
Conectar áreas de almacenamiento de datos de vSphere 41
Optimizar vSphere para XtremIO 42
Implementación de EMC Virtual Storage Integrator 43
Optimización de hosts de vSphere para XtremIO 45
Instalación y configuración de la base de datos de SQL Server 47
Implementación de VMware vCenter Server 49
Configurar View Connection Server 50
Instalar View Connection Server 51
Configurar la conexión de la base de datos de registros de eventos de Horizon View 51
Agregar una réplica de la instancia de View Connection Server 51
Configurar la conexión ODBC de View Composer 51
Instalar View Composer 52
Conectar Horizon View a vCenter y View Composer 52
Preparar una máquina virtual maestra 52
Configurar políticas de grupo de Horizon View Persona Management 53
Configurar las políticas de grupo de redireccionamiento de carpetas para EMC Avamar 53
Configurar políticas de grupo de PCoIP de Horizon View 53
Provisionar escritorios virtuales con View Composer 53
Provisionar escritorios virtuales con VSI 55
Recuperación del espacio de la capacidad física de XtremIO 56
Consideraciones de la operación SCSI UNMAP 57
Uso de un script para ejecutar las operaciones SCSI UNMAP 57
Uso de EMC VSI para ejecutar las operaciones SCSI UNMAP 59
Configurar el respaldo y la recuperación de EMC Avamar 60
Configurar VMware vShield Endpoint 60
Verificar la instalación del controlador de vShield Endpoint en los escritorios 61
Implementar el dispositivo vShield Manager 61
Instalar el servicio vShield Endpoint 61
Implementar un servidor de administración de la solución antivirus 62
Implementar máquinas virtuales de seguridad de vSphere 62

Verificar la funcionalidad de vShield Endpoint....62
Configurar VMware Workspace....62
Crear un nuevo pool de IP de vCenter....66
Asignar direcciones IP y crear registros DNS....66
Otorgar permisos de retransmisión SMTP de VMware Workspace....66
Configurar una base de datos de PostgreSQL u Oracle para VMware Workspace....66
Configurar un recurso compartido CIFS para usar como catálogo de ThinApp (opcional)....66
Verificar que todos los usuarios de VMware Workspace tengan una dirección de correo electrónico especificada....66
Implementar la vApp de VMware Workspace en vCenter....67
Ajustar las especificaciones de la máquina virtual de VMware Workspace....67
Obtener la información requerida para permitir la integración de VMware Workspace en Active Directory....67
Obtener un certificado SSL de confianza y la clave privada para las máquinas virtuales de VMware Workspace (opcional)....68
Configurar el acceso externo al gateway de VMware Workspace (opcional)....68
Activar la integración de Horizon View (opcional)....68
Configurar VMware vRealize Operations Manager for Horizon View....68

Capítulo 5 Verificación de la solución 71

Descripción general....72
Lista de verificación posterior a la instalación....73
Implementar y probar una sola máquina virtual....73
Verificar la redundancia de los componentes de la solución....73
XtremIO....73
Isilon....74
VNX74
Host de vSphere....75

Capítulo 6 Documentación de referencia 77

Documentación de EMC....78
Otra documentación....78

Apéndice A Hoja de trabajo de configuración 81

Hoja de trabajo de configuración del cliente....82

Figuras

Figura 1. Infraestructuras comprobadas VSPEX 21
Figura 2. Arquitectura de la solución validada 22
Figura 3. Arquitectura lógica 23
Figura 4. Ejemplo de arquitectura de red Ethernet 28
Figura 5. Ejemplo de arquitectura de red Fibre Channel 29
Figura 6. Cuadro de diálogo Storage System Properties 33
Figura 7. Cuadro de diálogo Create FAST Cache 34
Figura 8. Creación de un recurso compartido de SMB en Isilon 35
Figura 9. Cuadro de diálogo Storage Pool Properties 37
Figura 10. Cuadro de diálogo Manage Auto-Tiering 37
Figura 11. Opción Display Event Handlers de XtremIO 39
Figura 12. Cuadro de diálogo Edit Event Handler en XtremIO 39
Figura 13. vSphere Web Client: Integración con EMC VSI 44
Figura 14. vSphere Web Client: EMC VSI: sistemas de almacenamiento 44
Figura 15. vSphere Web Client: acciones del área de almacenamiento de datos de EMC VSI para XtremIO 45
Figura 16. vSphere Web Client: configuración del host de EMC VSI 46
Figura 17. vSphere Web Client: configuración del host de EMC VSI 46
Figura 18. Cuadro de diálogo de View Composer Disks 54
Figura 19. XtremIO Storage Management Application: gráfico de ancho de banda de rendimiento 58
Figura 20. EMC Storage Analytics: gráfico de las métricas de almacenamiento 58
Figura 21. vSphere Web Client: recuperación de espacio de almacenamiento no utilizado en EMC VSI 59
Figura 22. vSphere Web Client: detalles de la recuperación de espacio 59
Figura 23. vSphere Web Client: visualización de la pestaña Running en Recent Tasks 60

Tablas

Tabla 1. Terminología 12
Tabla 2. Tareas previas a la implementación 14
Tabla 3. Flujo de trabajo de implementación 15
Tabla 4. Lista de verificación de los requisitos previos de la implementación 16
Tabla 5. Componentes de la solución 24
Tabla 6. Descripción general del proceso de implementación 26
Tabla 7. Tareas para la configuración de los switches y la red 27
Tabla 8. Tareas para la configuración del almacenamiento 30
Tabla 9. Volúmenes en XtremIO para almacenar escritorios virtuales 32
Tabla 10. Configuración de un pool de almacenamiento RAID 6 basado en bloques 36
Tabla 11. Configuración de LUN para pool de NAS 36
Tabla 12. Requisitos mínimos del servidor de la infraestructura 38

Tabla 13. Tareas para la instalación de servidores 40
Tabla 14. Tareas para la configuración de una base de datos de SQL Server 48
Tabla 15. Tareas para la configuración de vCenter 49
Tabla 16. Tareas para la configuración de View Connection Server 50
Tabla 17. Tareas requeridas para instalar y configurar vShield Endpoint 60
Tabla 18. Tareas para la configuración de VMware Workspace 62
Tabla 19. VMware Workspace para más de 1,000 usuarios: requisitos de recursos de hardware mínimos 67
Tabla 20. Tareas requeridas para instalar y configurar vRealize Operations Manager 68
Tabla 21. Tareas para comprobar la instalación 72
Tabla 22. Información común del servidor 82
Tabla 23. Información del servidor vSphere 82
Tabla 24. Información del arreglo XtremIO 83
Tabla 25. Información del arreglo VNX 83
Tabla 26. Información del arreglo Isilon 83
Tabla 27. Información de la infraestructura de red 84
Tabla 28. Información de VLAN 84
Tabla 29. Cuentas de servicio 84

Capítulo 1 Introducción

Este capítulo presenta los siguientes temas:

Propósito de esta guía 10

Valor para el negocio 10

Alcance 11

Audiencia 11

Terminología 12

Propósito de esta guía

La infraestructura comprobada de cómputo del usuario final de EMC® VSPEX® proporciona a los clientes un sistema moderno capaz de alojar una gran cantidad de escritorios virtuales con un nivel de rendimiento coherente. Esta solución de cómputo del usuario final de VSPEX con VMware Horizon View 6.0 se ejecuta en una capa de virtualización de VMware vSphere respaldada por la familia EMC XtremIO™ de alta disponibilidad, que proporciona el almacenamiento. En esta solución, los componentes de infraestructura de virtualización de escritorio están colocados en capas en una infraestructura comprobada de VSPEX Private Cloud for VMware vSphere, mientras que los escritorios se alojan en recursos exclusivos.

Los componentes de cómputo y de red, definidos por los partners de VSPEX, están diseñados para que sean redundantes y lo bastante eficaces para manejar las necesidades de procesamiento y de datos de un amplio ambiente de máquinas virtuales. Los arreglos de EMC XtremIO proporcionan almacenamiento para escritorios virtuales; los arreglos EMC VNX® brindan almacenamiento para datos de usuarios; las opciones de respaldo y recuperación de EMC Avamar® brindan protección para datos de VMware Horizon View; y EMC RSA® SecurID® proporciona una funcionalidad opcional de autenticación de usuario segura.

Esta solución de cómputo del usuario final de VSPEX está validada para un máximo de 2,500 escritorios virtuales de clonación completa o 3,500 de clonación vinculada para un X-Brick, y hasta 1,250 escritorios virtuales de clonación completa o 1,750 de clonación vinculada para un Starter X-Brick. Estas configuraciones validadas están basadas en una carga de trabajo de escritorios de referencia y forman la base para soluciones rentables y personalizadas para clientes individuales.

XtremIO es compatible con clusters de escalamiento horizontal de hasta seis X-Brick. Cada X-Brick adicional aumenta el rendimiento y la capacidad de los escritorios virtuales de manera lineal. Los X-Brick de XtremIO se han validado para dar soporte a una mayor cantidad de escritorios (tanto de clonación completa como vinculada) y los números validados de VSPEX son exclusivos de la solución comunicada.

Un cómputo del usuario final o una infraestructura de escritorios virtuales es una oferta de sistema compleja. En esta guía de implementación se describe cómo implementar, con las mejores prácticas, los recursos necesarios para implementar una solución de cómputo del usuario final mediante Horizon View para VMware vSphere con tecnología de XtremIO, EMC Isilon®, VNX y EMC Data Protection.

Valor para el negocio

Las aplicaciones de negocio están migrando al ambiente consolidado de cómputo, red y almacenamiento. La solución de EMC VSPEX con VMware reduce la complejidad de configurar cada componente de un modelo de implementación tradicional. También simplifica la administración de la integración mientras mantiene las opciones de diseño e implementación de aplicaciones. Asimismo, proporciona una administración unificada mientras permite el control y el monitoreo adecuados de la separación de procesos.

Entre los beneficios para el negocio que ofrece la solución de cómputo del usuario final de VSPEX para VMware Horizon View se encuentran los siguientes:

- Una solución de virtualización de punto a punto para aprovechar las capacidades de los componentes de la infraestructura unificada
- Virtualización eficaz para diversos casos de uso de clientes
- Arquitecturas de referencia confiables, flexibles y escalables

Alcance

Esta guía de implementación describe los pasos generales necesarios para implementar la solución de cómputo del usuario final de VSPEX para VMware Horizon View 6.0. Proporciona un ejemplo de implementación de un almacenamiento de escritorios virtuales en XtremIO y un almacenamiento de datos de usuario en un arreglo de almacenamiento Isilon o VNX. Los servidores de infraestructura que requiere esta solución están diseñados para que sean colocados en capas en una infraestructura comprobada de VSPEX Private Cloud for VMware vSphere. Se aplican los mismos principios y reglas a los arreglos XtremIO, Isilon y VNX que se hayan validado como parte del programa de EMC VSPEX.

Las soluciones de EMC Data Protection para VMware Horizon View se describen en un documento aparte: *EMC Backup and Recovery for VSPEX for End-User Computing with VMware Horizon View: guía de diseño e implementación*.

La solución opcional para la autenticación segura de usuarios de RSA® SecurID® para VMware Horizon View se describe en otro documento: *Seguridad del cómputo del usuario final de EMC VSPEX con RSA SecurID: VMware Horizon View 5.2 y VMware vSphere 5.1 para hasta 2,000 escritorios virtuales: guía de diseño*.

Audiencia

Esta guía está dirigida al personal interno de EMC y a partners calificados de EMC VSPEX. En esta guía se supone que los partners de VSPEX que pretenden implementar esta infraestructura comprobada VSPEX para VMware Horizon View tienen la capacitación y la experiencia necesarias para instalar y configurar una solución de cómputo del usuario final basada en Horizon View con vSphere como el hipervisor, los sistemas de almacenamiento de las series XtremIO, Isilon y VNX, y la infraestructura relacionada.

Los lectores también deben estar familiarizados con las políticas de seguridad de la infraestructura y la base de datos de la instalación del cliente.

En esta guía se ofrecen referencias externas cuando corresponda. EMC recomienda que los partners que implementen esta solución conozcan estos documentos. Para obtener información detallada, consulte Lectura esencial y Documentación de referencia.

Terminología

La Tabla 1 detalla la terminología usada en esta guía.

Tabla 1. Terminología

Término	Definición
Deduplicación de datos	Una función del arreglo XtremIO que reduce la utilización del almacenamiento físico eliminando bloques de datos redundantes.
Clones completos	Escritorios que se implementan con una plantilla de vSphere.
Copias enlazadas	Escritorios que comparten una imagen base común dentro de un pool de escritorios y, como tales, tienen un espacio físico de almacenamiento mínimo.
Arquitectura de referencia	La arquitectura validada compatible con esta solución de cómputo del usuario final de VSPEX en cuatro puntos de escala específicos.
Carga de trabajo de referencia	Para las soluciones de cómputo del usuario final de VSPEX, un solo escritorio virtual (el escritorio virtual de referencia) con la configuración de la carga de trabajo que se indica en la guía de diseño. Al comparar el uso real del cliente con la carga de trabajo de referencia, puede decidir qué arquitectura de referencia debe elegir como base para la implementación de VSPEX. Consulte la guía de diseño para obtener información detallada.

Capítulo 2 Antes de comenzar

Este capítulo presenta los siguientes temas:

Descripción general 14

Tareas previas a la implementación 14

Flujo de trabajo de implementación 15

Lectura esencial 15

Prerrequisitos de la implementación 16

Descripción general

Este capítulo proporciona una descripción general de la información importante y los documentos que necesita conocer, además de las tareas que debe realizar antes de comenzar con la implementación de la solución de cómputo del usuario final de VSPEX para VMware Horizon View.

El documento complementario para esta solución, *Cómputo del usuario final de EMC VSPEX: VMware Horizon View 6.0 y VMware vSphere con EMC XtremIO: guía de diseño*, describe cómo dimensionar y diseñar la solución, asignar recursos de acuerdo con las mejores prácticas y utilizar todos los beneficios que VSPEX ofrece. Los ejemplos de implementación de esta Guía de implementación se basan en las recomendaciones y los ejemplos de la Guía de diseño.

Tareas previas a la implementación

Las tareas previas a la implementación incluyen procedimientos que no se relacionan directamente con la instalación y la configuración del ambiente, pero cuyos resultados serán necesarios en el momento de la instalación. Algunos ejemplos de tareas previas a la implementación son la recopilación de nombres de host, direcciones IP, ID de VLAN, números de licencia, medios de instalación, etc. Estas tareas deben realizarse antes de visitar a un cliente para disminuir el tiempo necesario en el sitio.

Tabla 2. Tareas previas a la implementación

Tarea	Descripción	Referencia
Reunir documentos	Reúna los documentos relacionados que aparecen en Lectura esencial y en Documentación de referencia. Estos se usan en toda esta guía de implementación para proporcionar detalles sobre procedimientos de configuración, dimensionamiento y mejores prácticas de implementación para los diversos componentes de la solución.	• Lectura esencial • Documentación de referencia
Reunir herramientas	Reúna las herramientas requeridas y opcionales para la implementación. Use la Tabla 4, en la página 16, para comprobar que todos los equipos, el software y las licencias correspondientes estén disponibles antes del proceso de implementación.	Tabla 4, Lista de verificación de los requisitos previos de la implementación
Recopilar datos	Recopile datos de configuración específicos del cliente sobre redes, arreglos, cuentas, etc. Ingrese esta información en la Hoja de trabajo de configuración del cliente para usarla como referencia durante el proceso de implementación. Además, para obtener la información específica sobre el arreglo más completa posible, complete la lista de verificación previa a la instalación de XtremIO y la hoja de trabajo de VNX pertinentes. Estos documentos están disponibles en el servicio de soporte en línea de EMC.	• *EMC XtremIO Storage Array Pre-Installation Checklist* • *EMC VNX Installation Assistant for File/Unified Worksheet* • Hoja de trabajo de configuración del cliente

Flujo de trabajo de implementación

Para diseñar e implementar su solución de cómputo del usuario final, consulte el flujo de proceso en la Tabla 3.

Tabla 3. Flujo de trabajo de implementación

Paso	Acción
1	Use la hoja de trabajo de dimensionamiento del cliente que se incluye en la guía de diseño para recopilar los requisitos del cliente.
2	Use la herramienta para dimensionamiento de EMC VSPEX para determinar la arquitectura de referencia de VSPEX recomendada para la solución de cómputo del usuario final, según los requisitos del usuario recopilados en el paso 1. Para obtener más información acerca de la herramienta para dimensionamiento, consulte Herramienta para dimensionamiento de VSPEX. **Nota**: Si la herramienta para dimensionamiento no está disponible, puede dimensionar manualmente la aplicación de acuerdo con las reglas de la guía de diseño.
3	Utilice la Guía de diseño para determinar el diseño final para su solución VSPEX. **Nota**: Asegúrese de considerar todos los requisitos de recursos y no solo los requisitos para el cómputo del usuario final.
4	Seleccione y solicite la infraestructura comprobada y la arquitectura de referencia de VSPEX correspondientes. Consulte el documento *Nube privada de EMC VSPEX: VMware vSphere 5.5 para hasta 1,000 máquinas virtuales: guía de infraestructura comprobada* para obtener orientación sobre la selección de una infraestructura comprobada de nube privada de VSPEX.
5	Siga esta guía de implementación para implementar y probar la solución VSPEX. **Nota**: Si ya tiene un ambiente de infraestructura comprobada VSPEX, puede omitir los pasos de implementación que ya se completaron.

Lectura esencial

EMC recomienda leer los siguientes documentos, disponibles en el espacio de VSPEX en EMC Community Network, en mexico.emc.com (visite el sitio web de su país correspondiente) o el portal para partners de la infraestructura comprobada VSPEX.

Descripción general de la solución VSPEX

Consulte *Soluciones de cómputo del usuario final de EMC VSPEX con VMware vSphere y VMware View: descripción general de la solución* para obtener más información general acerca de la solución VSPEX.

Guía de diseño de VSPEX

Consulte *Cómputo del usuario final de EMC VSPEX: VMware Horizon View 6.0 y VMware vSphere con EMC XtremIO: guía de diseño* para obtener más información.

Guía de la infraestructura comprobada VSPEX

Consulte el documento *Nube privada de EMC VSPEX: VMware vSphere 5.5 para hasta 1,000 máquinas virtuales: guía de infraestructura comprobada* para obtener más información sobre una infraestructura comprobada VSPEX.

Guía de respaldo y recuperación de EMC para VSPEX

Consulte *EMC Backup and Recovery for VSPEX for End-User Computing with VMware Horizon View: guía de diseño e implementación* para obtener más información sobre EMC Data Protection para VSPEX.

Prerrequisitos de la implementación

En la Tabla 4 se detallan los requisitos de hardware, software y licencias para configurar la solución. Visite el servicio de soporte en línea de EMC para obtener más información sobre estos requisitos previos.

Tabla 4. Lista de verificación de los requisitos previos de la implementación

Requisito	Descripción
Hardware	• Servidores físicos con capacidad suficiente para alojar escritorios virtuales según las recomendaciones de la guía de diseño • Servidores de VMware vSphere para alojar servidores de infraestructura virtual • Capacidad y funcionalidades de puerto de switch de redes según los requisitos del cómputo del usuario final • Arreglo de EMC XtremIO con la configuración necesaria • EMC Isilon con la configuración requerida • Arreglo de almacenamiento multiprotocolo EMC VNX con el diseño de disco requerido **Nota**: Estos requisitos se pueden cumplir con la infraestructura existente.
Software	• Medios de instalación de VMware vSphere 5.5 • Medios de instalación de VMware vCenter Server 5.5 • Archivo de dispositivo de virtualización de código abierto (OVA) de VMware vShield Manager • Archivo OVA de VMware vRealize Operations Manager • Adaptador de VMware vRealize Operations Manager for Horizon View • Medios de instalación de VMware Horizon View 6.0 • Software de servidor de administración de la solución antivirus partner de VMware vShield Endpoint • Software de máquina virtual de seguridad partner de VMware vShield Endpoint • Archivo OVA de EMC XtremIO Management Server • EMC Virtual Storage Integrator (VSI) para el cliente web de VMware vSphere • EMC VSI para VMware vSphere: Storage Viewer • EMC PowerPath® Viewer • EMC PowerPath/VE. • Medios de instalación de Microsoft Windows Server 2012 R2 (SO sugerido para VMware vCenter y VMware Horizon View Connection Server) • Medios de instalación de Microsoft Windows 7 o Windows 8.1 • Medios de instalación de Microsoft SQL Server 2012 o superior **Nota**: Este requisito se puede cubrir con la infraestructura existente.

Requisito	Descripción
Licencias	• Números de licencia de VMware vSphere 5.5 (para los hosts de servidores de infraestructura) • Número de licencia de VMware vCenter Server 5.5 • Números de licencia de VMware vSphere Desktop (para los hosts de escritorios virtuales) • Número de licencia de VMware Horizon View 6.0 • Números de licencia de VMware vShield Endpoint (VMware) • Números de licencia de VMware vShield Endpoint (partner de vShield) • Número de licencia de VMware vRealize Operations Manager • Números de licencia de Microsoft Windows Server 2012 R2 Standard Edition (o superior) • Números de licencia de Microsoft Windows 7 o Windows 8.1 • Número de licencia de Microsoft SQL Server 2012 **Nota**: Estos requisitos de licencia se pueden cumplir con el servidor de administración de claves (KMS) de Microsoft existente u otras licencias. • Archivos de licencia de EMC PowerPath/VE

Capítulo 3 descripción general de la solución

Este capítulo presenta los siguientes temas:

Descripción general **20**

Infraestructuras comprobadas VSPEX **20**

Arquitectura de la solución **21**

Resumen de los componentes clave **24**

Descripción general

En este capítulo se proporciona una descripción general de la solución de cómputo del usuario final de VSPEX para VMware Horizon View y VMware vSphere y las tecnologías clave que se usan en la solución. EMC diseñó y comprobó la solución para proporcionar los recursos de virtualización de escritorios, servidores, redes, almacenamiento y respaldo para dar soporte a las arquitecturas de referencia de hasta 2,500 escritorios virtuales de clonación completa o 3,500 de clonación vinculada para un X-Brick, y hasta 1,250 escritorios virtuales de clonación completa o 1,750 de clonación vinculada para un Starter X-Brick.

Los X-Brick de XtremIO se validaron para dar soporte a una mayor cantidad de escritorios, tanto de clonación completa como vinculada. Los números validados de VSPEX son exclusivos de la solución comunicada.

Aunque los componentes de infraestructura de virtualización de escritorio de la solución que se muestran en la Figura 3 de la página 23 están diseñados para colocarse en capas en una solución de nube privada de VSPEX, las arquitecturas de referencia no incluyen detalles de configuración para la infraestructura comprobada subyacente. Consulte el documento *Nube privada de EMC VSPEX: VMware vSphere 5.5 para hasta 1,000 máquinas virtuales: guía de infraestructura comprobada* para obtener información sobre cómo configurar los componentes requeridos de la infraestructura.

Infraestructuras comprobadas VSPEX

EMC aunó fuerzas con los proveedores de infraestructuras de TI para crear una solución de virtualización completa que agilice la implementación de la nube privada y de los escritorios virtuales de VMware Horizon View. VSPEX permite que los clientes aceleren su transformación de TI mediante una implementación más rápida, más simple, con más opciones, mayor eficiencia y menor riesgo, en comparación con los retos y la complejidad de construir una infraestructura de TI por sí mismos.

La validación de VSPEX por parte de EMC garantiza un rendimiento predecible y les permite a los clientes seleccionar una tecnología que utilice su infraestructura de TI existente o recién adquirida mientras eliminan las tareas de planificación, dimensionamiento y configuración. VSPEX proporciona una infraestructura virtual para los clientes que desean obtener la simplicidad característica de las infraestructuras realmente convergentes y disponer de más opciones en los componentes agrupados individuales.

Las infraestructuras comprobadas VSPEX, como se muestra en la Figura 1, corresponden a infraestructuras modulares virtualizadas, validadas por EMC y suministradas por los partners de EMC VSPEX. Incluyen capas de virtualización, servidor, red, almacenamiento y respaldo. Los partners pueden elegir las tecnologías de virtualización, de servidor y de red que mejor se ajusten al ambiente del cliente, a la vez que los sistemas de almacenamiento XtremIO, Isilon y VNX de alta disponibilidad y las tecnologías de EMC Data Protection proporcionan las capas de almacenamiento y de respaldo.

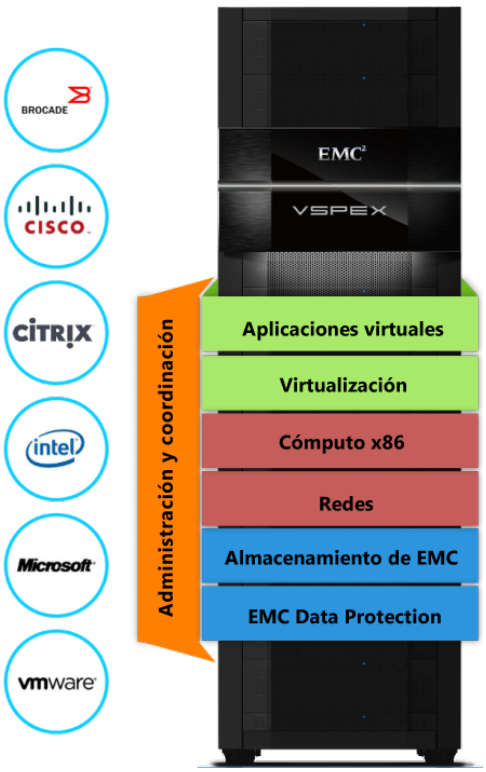


Figura 1. Infraestructuras comprobadas VSPEX

Arquitectura de la solución

Arquitectura de alto nivel

La solución de cómputo del usuario final de EMC VSPEX para VMware Horizon View proporciona una arquitectura del sistema completa con dos configuraciones de X-Brick de XtremIO. Un X-Brick es capaz de dar soporte a un máximo de 2,500 escritorios virtuales de clonación completa o 3,500 de clonación vinculada, y un Starter X-Brick puede admitir un máximo de 1,250 escritorios virtuales de clonación completa o 1,750 de clonación vinculada. La solución es compatible con el almacenamiento de bloques en XtremIO para escritorios virtuales y almacenamiento de archivos opcional en Isilon o VNX para los datos de usuario.

La Figura 2 describe la arquitectura general de la solución validada.

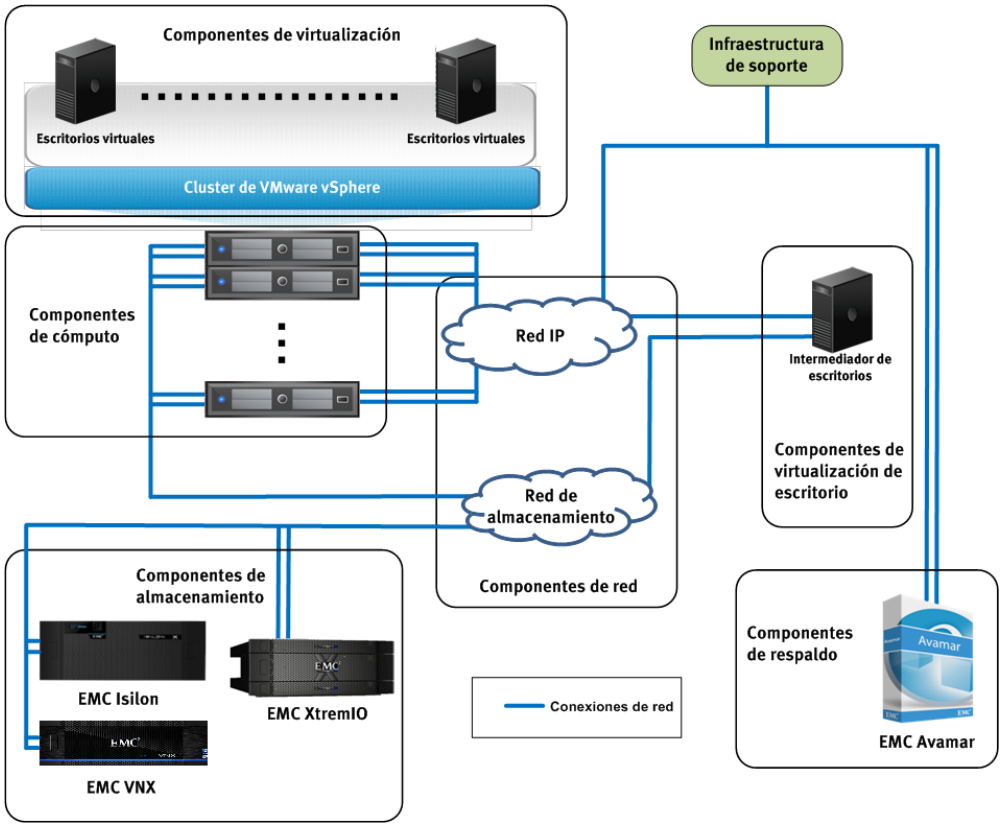


Figura 2. Arquitectura de la solución validada

La solución usa XtremIO, Isilon o VNX, y vSphere para proporcionar las plataformas de almacenamiento y de virtualización para un ambiente de Horizon View de escritorios virtuales de Microsoft Windows 7 o Windows 8.1 provisionados por VMware View Composer.

Para la solución, implementamos[1] el arreglo XtremIO en varias configuraciones para ser compatible con hasta 3,500 escritorios virtuales. Hicimos pruebas con los siguientes arreglos XtremIO:

- Un Starter X-Brick, que se usó para alojar 1,250 escritorios virtuales de clonación completa o 1,750 de clonación vinculada
- Un X-Brick completo, que se usó para alojar 2,500 escritorios virtuales de clonación completa o 3,500 de clonación vinculada

También implementamos un cluster de Isilon y un arreglo VNX para alojar datos de usuario.

Los servicios de infraestructura para la solución, como se muestra en la Figura 3, pueden ser proporcionados por la infraestructura existente en el sitio del cliente, por la nube privada de VSPEX o mediante la implementación como recursos exclusivos como parte de la solución. Los escritorios virtuales requieren recursos de cómputo del usuario final exclusivos y no están diseñados para ser colocados en capas en VSPEX Private Cloud.

[1] En esta guía, cuando se habla de “nosotros” o “en nuestro caso” se hace referencia al equipo de ingeniería de EMC VSPEX que validó la solución.

La planificación y el diseño de la infraestructura de almacenamiento para un ambiente Horizon View es un paso crítico debido a que el almacenamiento compartido debe poder absorber los altos picos de I/O que ocurren en el transcurso de una jornada. Estas ráfagas pueden dar lugar a períodos de rendimiento errático e impredecible de los escritorios virtuales. Los usuarios pueden adaptarse a un rendimiento lento, pero el rendimiento impredecible crea frustración y reduce la eficiencia.

Para proporcionar un rendimiento predecible para las soluciones de cómputo del usuario final, el sistema de almacenamiento debe poder manejar la carga máxima de I/O de los clientes y mantener el tiempo de respuesta al mínimo. Esta solución usa el arreglo XtremIO para proporcionar los tiempos de respuesta inferiores al milisegundo que los clientes requieren, a la vez que reduce la cantidad de almacenamiento físico necesario gracias a las funciones de deduplicación en línea en tiempo real de la plataforma.

Las soluciones de EMC Data Protection permiten la protección de datos del usuario y la capacidad de recuperación de los usuarios finales. Esta solución de Horizon View utiliza el respaldo y la recuperación de Avamar y su cliente de escritorio para lograr esto.

Arquitectura lógica

Esta solución es compatible con el almacenamiento de bloques para los escritorios virtuales. La Figura 3 muestra la arquitectura lógica de la solución.

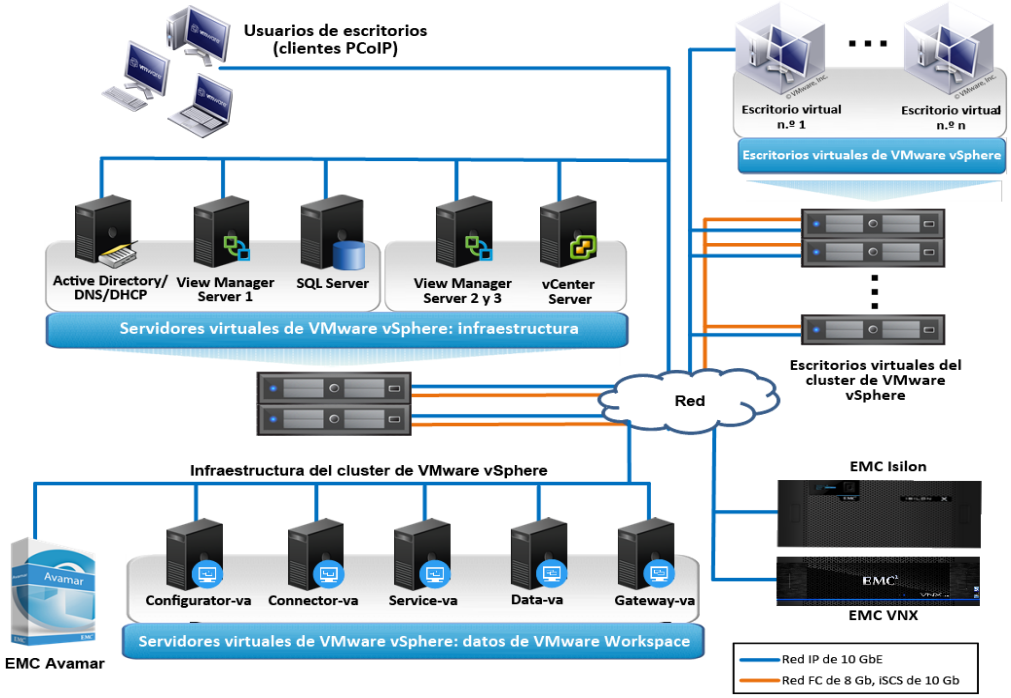


Figura 3. Arquitectura lógica

Esta solución utiliza dos redes: una red de almacenamiento para transportar los datos del SO del servidor virtual y de los escritorios virtuales, y una red de 10 Gb Ethernet (GbE) para transportar el resto del tráfico. La red de almacenamiento utiliza un Fibre Channel (FC) de 8 Gb, o bien, una red de 10 GbE con protocolo iSCSI.

Nota: Esta solución también es compatible con la red de 1 GbE si se cumplen los requisitos de ancho de banda.

Resumen de los componentes clave

La Tabla 5 resume las tecnologías clave que se usan en esta solución. La Guía de diseño proporciona descripciones generales de cada componente.

Tabla 5. Componentes de la solución

Capa de VSPEX	Componentes
Capa de aplicaciones	• Gestor de virtualización de escritorios VMware Horizon View 6.0 con lo siguiente: ▪ VMware View Manager ▪ VMware View Composer ▪ VMware Horizon View Persona Management ▪ VMware Horizon View Storage Accelerator ▪ VMware vRealize Operations Manager for Horizon View • Espacio de trabajo de VMware
Capa de virtualización	• Hipervisor VMware vSphere con lo siguiente: ▪ VMware vSphere ▪ VMware vCenter Server ▪ Alta disponibilidad de VMware vSphere • VMware vShield Endpoint
Capa de cómputo	Cualquier hardware de servidor que cumpla con los requisitos mínimos definidos por VSPEX
Capa de red	Cualquier hardware de red que cumpla con los requisitos mínimos definidos por VSPEX **Nota**: VSPEX define la cantidad mínima de puertos de red requeridos para la solución y proporciona orientación general sobre la arquitectura de red.
Capa de almacenamiento	• Serie EMC XtremIO con lo siguiente: ▪ EMC XtremIO Management Server ▪ EMC Virtual Storage Integrator (VSI) para el cliente web de VMware vSphere ▪ API de VMware vSphere Storage para integración de arreglos ▪ EMC XtremIO Snapshots • Serie EMC VNX con lo siguiente: ▪ EMC Unisphere® Management Suite ▪ EMC VSI para VMware vSphere ▪ API de VMware vSphere Storage para integración de arreglos ▪ API de almacenamiento de VMware vSphere para conciencia de almacenamiento ▪ EMC VNX Snapshots ▪ EMC SnapSure™ ▪ EMC VNX Virtual Provisioning ▪ EMC Fully Automated Storage Tiering (FAST™) Suite: FAST Cache y FAST for Virtual Pools (FAST VP)
Capa de respaldo y recuperación	EMC Avamar
Capa de seguridad	EMC RSA SecurID

Capítulo 4 Implementación de la solución

Este capítulo presenta los siguientes temas:

Descripción general 26
Implementación de la infraestructura de red 27
Preparación y configuración de los arreglos de almacenamiento 30
Instalación y configuración de los hosts vSphere 40
Instalación y configuración de la base de datos de SQL Server 47
Implementación de VMware vCenter Server 49
Configurar View Connection Server 50
Provisionar escritorios virtuales con View Composer 53
Provisionar escritorios virtuales con VSI 55
Recuperación del espacio de la capacidad física de XtremIO 56
Configurar el respaldo y la recuperación de EMC Avamar 60
Configurar VMware vShield Endpoint 60
Configurar VMware Workspace 62
Configurar VMware vRealize Operations Manager for Horizon View 68

Descripción general

En este capítulo se describe cómo implementar la arquitectura de referencia de la solución de cómputo del usuario final. Si ya cuenta con un ambiente de infraestructura comprobada VSPEX, puede omitir las secciones con los pasos de implementación ya completados. De lo contrario, consulte *Nube privada de EMC VSPEX: VMware vSphere 5.5 para hasta 1,000 máquinas virtuales: guía de infraestructura comprobada* para obtener información sobre cómo configurar los componentes requeridos de la infraestructura.

Nota: Esta solución requiere ciertos servicios de infraestructura, como se muestra en la Figura 3, en la página 23. Pueden ser proporcionados por la infraestructura existente en el sitio del cliente, por VSPEX Private Cloud o mediante su implementación como recursos exclusivos de esta solución.

La Tabla 6 enumera las etapas principales del proceso de implementación de la solución y ofrece vínculos a las secciones pertinentes en el capítulo.

Tabla 6. Descripción general del proceso de implementación

Etapa	Descripción	Referencia
1	Configurar los switches y las redes, y conectarse a la red del cliente.	Implementación de la infraestructura de red
2	Instalar y configurar los arreglos de XtremIO y VNX.	Preparación y configuración de los arreglos de almacenamiento
3	Configurar áreas de almacenamiento de datos de máquinas virtuales.	
4	Instalar y configurar los servidores.	Instalación y configuración de los hosts vSphere
5	Configurar SQL Server (utilizado por vCenter y Horizon View).	Instalación y configuración de la base de datos de SQL Server
6	Instalar y configurar vCenter y la red de máquinas virtuales.	Implementación de VMware vCenter Server
7	Configurar VMware View Connection Server.	Configurar View Connection Server
8	Provisionar escritorios virtuales.	Provisionar escritorios virtuales
9	Configurar EMC Avamar.	Configurar el respaldo y la recuperación
10	Configurar vShield Endpoint.	Configurar VMware vShield Endpoint
11	Configurar VMware Workspace.	Configurar VMware
12	Configurar VMware vRealize Operations Manager for Horizon View.	Configurar VMware vRealize Operations Manager for

Implementación de la infraestructura de red

En esta sección encontrará los requisitos para preparar la infraestructura de red requerida para que sea compatible con esta solución. La Tabla 7 resume las tareas que se realizarán e incluye referencias para obtener más información.

Tabla 7. Tareas para la configuración de los switches y la red

Tarea	Descripción	Referencia
Configurar la red de la infraestructura	Configure el arreglo de almacenamiento y la red de infraestructura de host vSphere.	Configurar la red de la infraestructura
Configuración de las VLAN	Configure VLAN privadas y públicas según sea necesario.	Guía de configuración de switches del proveedor
Configurar la red de almacenamiento	Configure los puertos del switch de Fibre Channel, la zonificación para hosts vSphere y el arreglo de almacenamiento.	• Configurar la red de almacenamiento • Guía de configuración de switches del proveedor
Conectar el cableado de la red	Conecte los puertos de interconexión de los switches, los puertos de VNX, los puertos de Isilon y los puertos del servidor vSphere.	Conectar el cableado de la red

Configurar la red de la infraestructura

La red de la infraestructura requiere vínculos de red redundantes para cada host vSphere, el arreglo de almacenamiento, los puertos de interconexión de los switches y los puertos de vínculo de subida de los switches. Esta configuración proporciona redundancia y ancho de banda de red adicional.

Esta configuración se requiere, sin importar si la infraestructura de red para la solución existe o se está implementando junto con otros componentes de la solución.

La Figura 4 muestra un ejemplo de infraestructura Ethernet redundante para el VNX usado en esta solución. Esta solución usa switches y vínculos redundantes para asegurarse de que no existan puntos únicos de falla en la conectividad de la red. Se aplica el mismo principio a una configuración de Isilon.

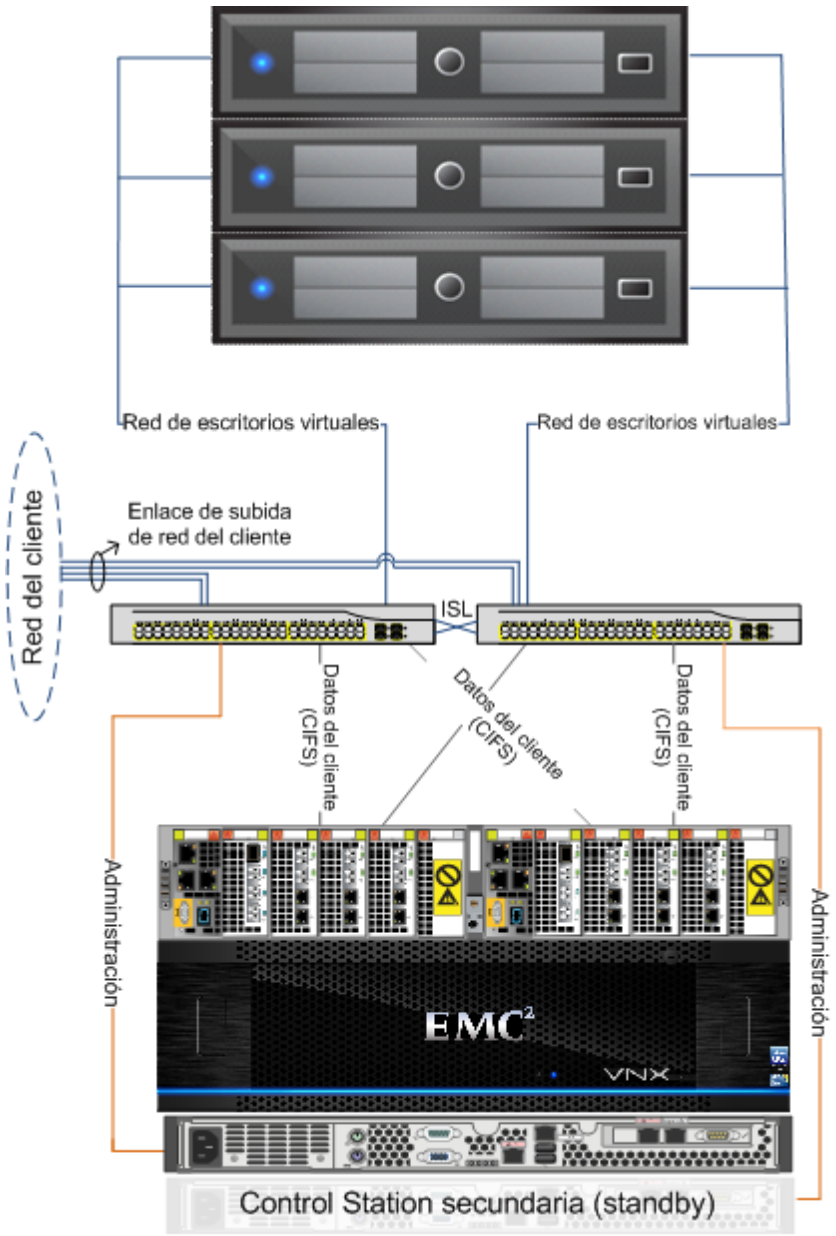


Figura 4. Ejemplo de arquitectura de red Ethernet

Configuración de las VLAN

Asegúrese de que la infraestructura incluya una cantidad adecuada de puertos de switch para el arreglo de almacenamiento y para los hosts de vSphere. EMC recomienda configurar los siguientes hosts vSphere con un mínimo de tres VLAN:

- **Red de acceso para clientes**: red de máquinas virtuales y tráfico CIFS (son redes para el cliente, que se pueden separar, si se desea)
- **Red de administración**: Administración de vSphere y VMware vMotion (red privada)

Configurar la red de almacenamiento

Esta solución requiere una red de almacenamiento exclusiva. Si iSCSI se utiliza para conectar hosts vSphere con el arreglo XtremIO, se requiere una VLAN exclusiva para la red de almacenamiento. Si se utiliza Fibre Channel o una combinación de Fibre Channel para el arreglo XtremIO y FCoE para los hosts de vSphere, no se requieren VLAN adicionales para la red de almacenamiento.

Para las pruebas de la solución, utilizamos una red Fibre Channel. La red Fibre Channel de la infraestructura requiere switches y vínculos Fibre Channel redundantes para cada host vSphere y para el arreglo de almacenamiento. Esta configuración proporciona redundancia y ancho de banda de red de almacenamiento adicional. Cada host vSphere se conectó a ambos switches FC y cada switch se conectó a cada procesador de almacenamiento en el arreglo de almacenamiento. Luego, se colocó cada conexión Fibre Channel entre el host vSphere y el arreglo de almacenamiento en una zona FC por separado.

La Figura 5 muestra la arquitectura de red utilizada para probar esta solución.

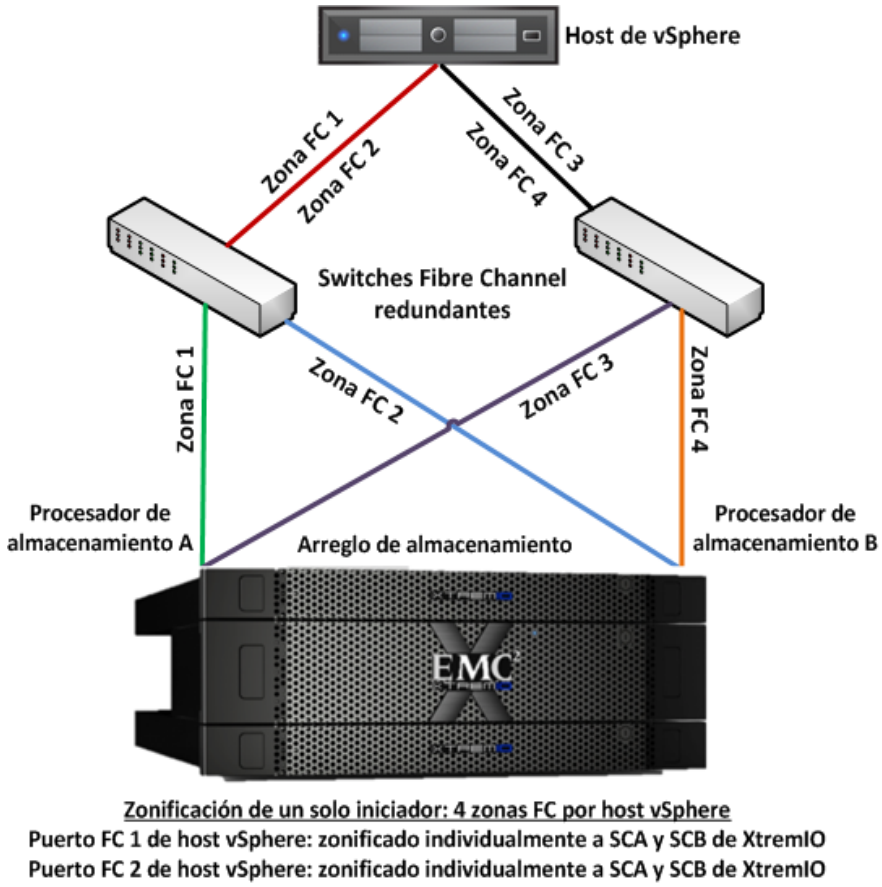

Host de vSphere
Zona FC 1
Zona FC 2
Zona FC 3
Zona FC 4
Switches Fibre Channel redundantes
Zona FC 1
Zona FC 2
Zona FC 3
Zona FC 4
Procesador de almacenamiento A
Arreglo de almacenamiento
Procesador de almacenamiento B
Zonificación de un solo iniciador: 4 zonas FC por host vSphere
Puerto FC 1 de host vSphere: zonificado individualmente a SCA y SCB de XtremIO
Puerto FC 2 de host vSphere: zonificado individualmente a SCA y SCB de XtremIO

Figura 5. Ejemplo de arquitectura de red Fibre Channel

Conectar el cableado de la red

Asegúrese de que todos los servidores, los arreglos de almacenamiento, las interconexiones de switches y los vínculos superiores de switches de la solución tengan conexiones redundantes y se conecten a infraestructuras de conmutación por separado. Asegúrese también de que haya una conexión completa con la red existente del cliente.

Nota: Después de verificar que el equipo nuevo esté conectado a la red existente del cliente, asegúrese de que las interacciones inesperadas no causen problemas de servicio en la red del cliente.

Preparación y configuración de los arreglos de almacenamiento

Esta sección describe cómo configurar los arreglos de almacenamiento XtremIO, Isilon y VNX usados en esta solución. El arreglo XtremIO proporciona almacenamiento de datos de VMware Virtual Machine File System (VMFS) para hosts VMware, mientras que el arreglo opcional VNX o Isilon brinda almacenamiento CIFS para datos de usuarios.

Todos los ejemplos de configuración de almacenamiento que se describen en este capítulo corresponden a las configuraciones de dos X-Brick validadas en esta solución. Para obtener información sobre configuraciones de mayor tamaño, comuníquese con su representante de ventas de EMC.

La Tabla 8 muestra las tareas correspondientes a la configuración del almacenamiento.

Tabla 8. Tareas para la configuración del almacenamiento

Tarea	Descripción	Referencia
Preparación de XtremIO	Instale el hardware XtremIO según lo indicado en la documentación del producto.	*EMC XtremIO Storage Array Hardware Installation and Upgrade Guide*
Preparar el cluster de Isilon	Instale el hardware de Isilon según lo indicado en la documentación del producto.	*Isilon Site Preparation and Planning Guide*
Preparar el VNX.	Instale el hardware VNX según lo indicado en la documentación del producto.	*Guía de infraestructura comprobada de la nube privada de VSPEX.*
Establecer la configuración inicial de XtremIO	Configure la información de direcciones IP y otros parámetros clave en XtremIO.	*EMC XtremIO Storage Array Software Installation and Upgrade Guide*
Establecer la configuración inicial de Isilon	Configure la información de direcciones IP y otros parámetros clave en Isilon.	*Isilon Site Preparation and Planning Guide*
Establecer la configuración inicial de VNX	Configure la información de direcciones IP y otros parámetros clave en VNX.	*Guía de infraestructura comprobada de la nube privada de VSPEX.*
Provisionar almacenamiento para áreas de almacenamiento de datos de VMFS	Cree volúmenes de XtremIO que se presentarán a servidores vSphere como áreas de almacenamiento de datos VMFS que alojan los escritorios virtuales.	Provisionar almacenamiento para áreas de almacenamiento de datos de VMFS
Configurar FAST Cache	Configure FAST Cache. De manera opcional, configure FAST VP.	• Configurar VNX FAST Cache • Configurar FAST VP para los datos de usuario en VNX (opcional)

Tarea	Descripción	Referencia
Provisionar almacenamiento opcional para los datos de usuario	Cree sistemas de archivos CIFS que se usarán para almacenar perfiles de usuario de roaming y directorios de inicio.	Provisionar almacenamiento opcional para los datos de usuario
Provisionar almacenamiento opcional para las máquinas virtuales de la infraestructura	Cree áreas de almacenamiento de datos VMFS adicionales para alojar máquinas virtuales para Microsoft SQL Server, los controladores de dominio, vCenter Server y View Connection Server.	Provisionar almacenamiento para áreas de almacenamiento de datos de VMFS

Preparar el arreglo XtremIO

Esta solución no requiere pasos de configuración específicos para el arreglo XtremIO. Para obtener instrucciones sobre el ensamblaje, el montaje en rack, el cableado y el encendido del arreglo XtremIO, consulte los siguientes documentos:

- *Guía de preparación del sitio del arreglo de almacenamiento EMC XtremIO*
- *EMC XtremIO Storage Array Pre-Installation Checklist*
- *EMC XtremIO Storage Array Software Installation and Upgrade Guide*
- *EMC XtremIO Storage Array Hardware Installation and Upgrade Guide*

Preparar el cluster de Isilon

Esta solución no requiere pasos de configuración específicos para el cluster de Isilon. Para obtener instrucciones sobre el ensamblaje, el montaje en rack, el cableado y el encendido del cluster de Isilon, consulte los siguientes documentos:

- *Guía de instalación de X400*
- *Isilon Site Preparation and Planning Guide*

Preparar el arreglo VNX

Esta solución no requiere pasos de configuración específicos para el arreglo VNX. Para obtener instrucciones sobre el ensamblaje, el montaje en rack, el cableado y el encendido del arreglo VNX, consulte la guía de instalación de VNX pertinente.

Configurar el arreglo XtremIO inicial

Después de preparar el arreglo XtremIO, configure la información clave sobre el ambiente existente. Configure los siguientes elementos conforme a las políticas del centro de datos de TI del cliente y a la información de infraestructura existente:

- Sistema de nombre de dominio (DNS)
- Protocolo de hora de red (NTP)
- Interfaz de red XMS
- Interfaces de la red de almacenamiento
- Dirección IP de la red de almacenamiento

Configurar el cluster de Isilon inicial

Después de preparar el arreglo Isilon, configure la información clave sobre el ambiente existente. Configure los siguientes elementos conforme a las políticas del centro de datos de TI del cliente y a la información de infraestructura existente:

- Configuración de la red externa
- Zonas de SmartConnect
- Zonas de acceso

Los documentos de referencia que se enumeran en el Capítulo 6 contienen más información sobre cómo configurar la plataforma Isilon.

Configurar del arreglo VNX inicial

Después de preparar el arreglo VNX, configure la información clave sobre el ambiente existente. Configure los siguientes elementos conforme a las políticas de su centro de datos de TI y a la información de infraestructura existente:

- DNS
- NTP
- Interfaces de la red de almacenamiento
- Dirección IP de la red de almacenamiento
- Servicios de Common Internet File System (CIFS) y membresía de Microsoft Active Directory Domain

Los documentos de referencia que se especifican en la Tabla 8 en la página 16 proporcionan más información sobre cómo configurar la plataforma VNX. En la guía de diseño se proporciona información sobre el diseño de disco.

Provisionar almacenamiento para áreas de almacenamiento de datos de VMFS

Realice el procedimiento siguiente para configurar los volúmenes en el arreglo XtremIO con el fin de almacenar escritorios virtuales:

1. En EMC XtremIO Storage Management Application, seleccione **Configuration**.
2. En **Volume**, haga clic en **Add**.
3. En la ventana **Add New Volumes**, haga clic en **Add Multiple**.
4. En **Number of Volumes**, escriba la cantidad requerida de áreas de almacenamiento de datos de acuerdo con la configuración detallada en la Tabla 9.

Tabla 9. Volúmenes en XtremIO para almacenar escritorios virtuales

Configuración	Cantidad de volúmenes	Tamaño del volumen (TB)
1,250 escritorios virtuales de clonación completa	10	5
1,750 escritorios virtuales de clonación vinculada	14	1
2,500 escritorios virtuales de clonación completa	20	5
3,500 escritorios virtuales de clonación vinculada	28	1

5. En **Name**, escriba un nombre común de LUN.
6. En **Size**, elija un tamaño de 1 TB o 5 TB en función de la configuración, como se especifica en la Tabla 9. Luego, haga clic en **OK**.

Configurar VNX FAST Cache

Para ver y configurar FAST Cache en el pool de almacenamiento VNX para esta solución:

1. En Unisphere, haga clic en **Properties** y seleccione **Manage Cache**.
2. Seleccione **FAST Cache** en el cuadro de diálogo **Storage System Properties**, como se indica en la Figura 6.
3. Para crear FAST Cache:
   a. Haga clic en **Create** para abrir el cuadro de diálogo **Create FAST Cache**.

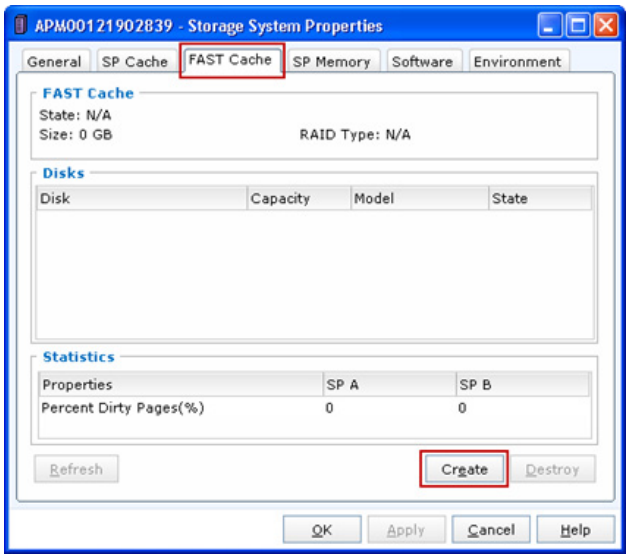


Figura 6. Cuadro de diálogo Storage System Properties

   b. Seleccione la cantidad necesaria de discos que han de usarse para FAST Cache.

   Si selecciona **Automatic**, el cuadro de diálogo mostrará una lista de discos flash que se utilizarán para crear FAST Cache.

   Para seleccionar las unidades manualmente, seleccione **Manual**.

   Para seleccionar el tipo de RAID, seleccione un valor de la lista desplegable, como se indica en la Figura 7. El valor predeterminado es 1.

Nota: Para determinar la cantidad de discos que se usará, consulte las reglas en la guía de diseño.

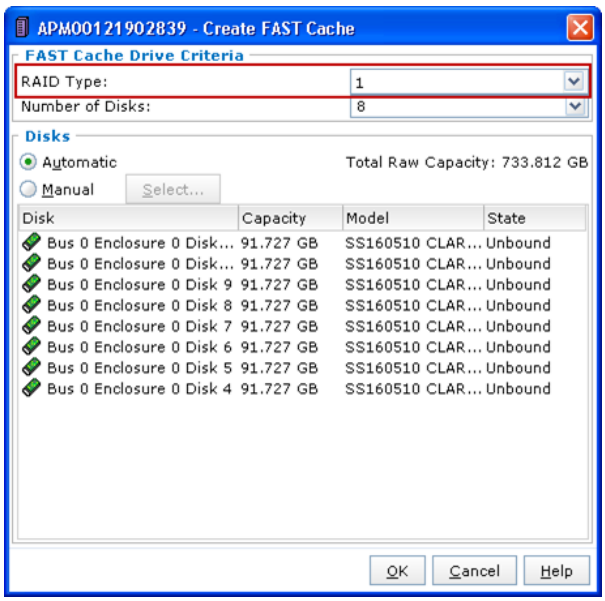

APM00121902839 - Create FAST Cache
FAST Cache Drive Criteria
RAID Type:
1
Number of Disks:
8
Disks
Automatic
Total Raw Capacity: 733.812 GB
Manual
Select...
Disk
Capacity
Model
State
Bus 0 Enclosure 0 Disk... 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk... 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 9 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 8 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 7 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 6 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 5 91.727 GB SS160510 CLAR... Unbound
Bus 0 Enclosure 0 Disk 4 91.727 GB SS160510 CLAR... Unbound
OK
Cancel
Help

Figura 7. Cuadro de diálogo Create FAST Cache

c. Haga clic en **OK** para crear FAST Cache.

Nota: Si no hay una cantidad suficiente de discos flash disponible, aparecerá un mensaje de error y FAST Cache no se creará.

Una vez creado FAST Cache, se activa de manera predeterminada para todos los pools que se creen posteriormente.

d. Para activar FAST Cache para el pool de almacenamiento existente creado para la solución, seleccione **FAST Cache Enabled** en **Avanced** en el cuadro de diálogo **Storage Pool Properties**.

La función FAST Cache en VNX no causa una mejora instantánea en el rendimiento. El sistema debe recopilar datos sobre patrones de acceso y promover la información de uso frecuente a la caché. Este proceso puede tardar algunas horas, durante las cuales el rendimiento del arreglo mejora constantemente.

Provisionar almacenamiento opcional para los datos de usuario

Isilon

Crear un solo recurso compartido de SMB común en Isilon para que lo utilicen todos los usuarios es la manera más fácil de configurar un ambiente de Microsoft Windows. Para esto, siga los pasos a continuación:

1. En la interfaz de administración web de OneFS, haga clic en **Protocols** › **Windows Sharing (SMB)**.
2. En la pestaña **SMB Shares**, haga clic en **Add a share.**
3. En el campo **Share Name**, ingrese el nombre de usuario (por ejemplo, Directorio principal).
4. En el campo **Directory to Be Shared**, ingrese la ruta completa correspondiente a la ubicación del directorio principal, comenzando con /ifs; o bien, haga clic en **Browse** para ubicar el directorio (por ejemplo, /ifs/home/).

5. Haga clic en **Create**.

   En la Figura 8 se muestra un ejemplo de cómo crear un recurso compartido de SMB.

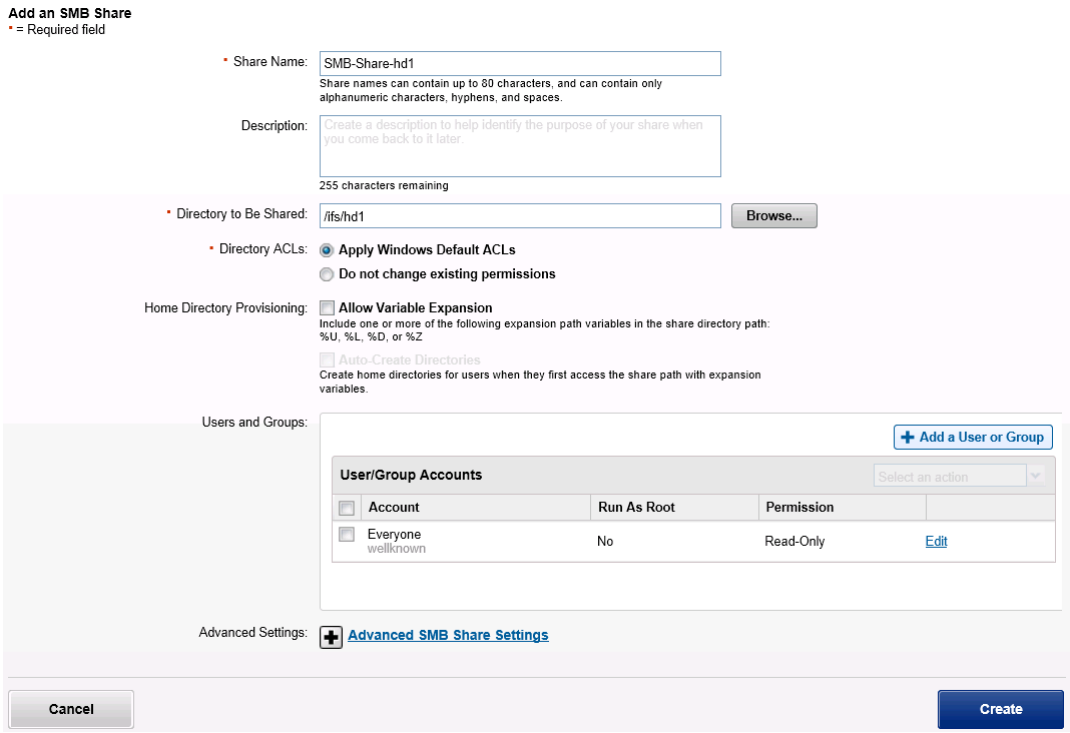

Add an SMB Share
* = Required field
* Share Name:
SMB-Share-hd1
Share names can contain up to 80 characters, and can contain only alphanumeric characters, hyphens, and spaces.
Description:
Create a description to help identify the purpose of your share when you come back to it later.
255 characters remaining
* Directory to Be Shared:
/ifs/hd1
Browse...
* Directory ACLs:
Apply Windows Default ACLs
Do not change existing permissions
Home Directory Provisioning:
Allow Variable Expansion
Include one or more of the following expansion path variables in the share directory path: %U, %L, %D, or %Z
Auto-Create Directories
Create home directories for users when they first access the share path with expansion variables.
Users and Groups:
Add a User or Group
User/Group Accounts
Select an action
Account
Run As Root
Permission
Everyone
wellknown
No
Read-Only
Edit
Advanced Settings:
Advanced SMB Share Settings
Cancel
Create

Figura 8. Creación de un recurso compartido de SMB en Isilon

De manera predeterminada, todos los usuarios tienen acceso al recurso compartido de SMB común y pueden acceder a los archivos de otros usuarios que tengan un directorio principal en dicho recurso compartido. Si desea definir permisos de acceso más estrictos, active la función de enumeración basada en acceso en Windows Server para mostrar en una lista solo los archivos y carpetas a los que cada usuario tiene acceso al navegar por contenido en el servidor de archivos.

Para obtener más información sobre otros métodos para configurar Isilon como el directorio principal, consulte *Managing SMB Shares and User Home Directories in EMC Isilon OneFS 6.5 and Later.*

VNX

Si el almacenamiento requerido para los datos de usuario (es decir, perfiles de usuario de roaming o repositorios de View Persona Management y directorios principales) todavía no existe en el ambiente de producción y se compró el paquete de discos de datos de usuario opcional, realice los siguientes pasos en Unisphere para configurar dos sistemas de archivos CIFS en VNX:

1. Cree un pool de almacenamiento basado en bloques RAID 6 con la configuración que se muestra en la Tabla 10.

Tabla 10. Configuración de un pool de almacenamiento RAID 6 basado en bloques

Configuración	Cantidad de unidades	Tipos de unidades
1,250 escritorios virtuales	16	SAS NL de 2 TB
1,750 escritorios virtuales	24	
2,500 escritorios virtuales	40	
3,500 escritorios virtuales	48	

En la guía de diseño se describen los diseños de almacenamiento.

2. Provisione los LUN requeridos del pool, como se puede ver en la Tabla 11, para presentarlos a Data Mover como dvols de un pool NAS definido por el sistema.

Tabla 11. Configuración de LUN para pool de NAS

Configuración	Cantidad de LUN	Tamaño del LUN (TB)
1,250 escritorios virtuales	10	1.5
1,750 escritorios virtuales	10	2.25
2,500 escritorios virtuales	10	3.75
3,500 escritorios virtuales	20	2.25

3. Provisione cuatro sistemas de archivos del pool NAS para exportar como recursos compartidos CIFS en un servidor CIFS.

Configurar FAST VP para los datos de usuario en VNX (opcional)

De manera opcional, puede configurar FAST VP para automatizar la transferencia de datos entre los niveles de almacenamiento en el pool de almacenamiento de datos del usuario. Es posible configurar FAST VP en el nivel del pool o de LUN.

Configuración de FAST VP en el nivel del pool

Para configurar FAST VP en el nivel del pool:

1. En Unisphere, seleccione el pool de almacenamiento para los datos de usuario y haga clic en **Properties**.
2. En **Storage Pool Properties**, seleccione **Tiering** para ver la información de la organización en niveles de un pool específico activado para FAST VP, como se muestra en la Figura 9.

   Tier Status muestra información de reubicación de FAST VP específica para el pool seleccionado. El panel **Tier Details** muestra la distribución exacta de los datos.

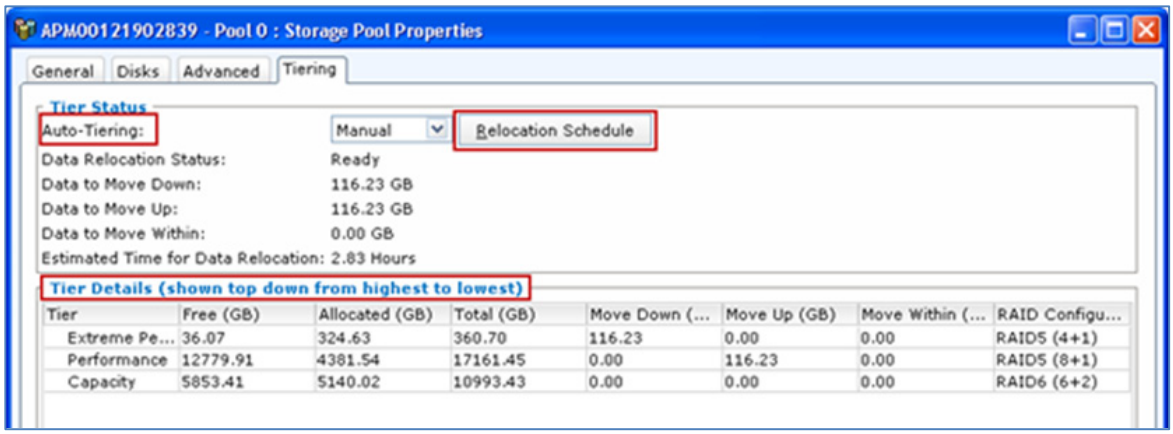


Figura 9. Cuadro de diálogo Storage Pool Properties

3. Configure **Auto-Tiering** en **Automatic** o **Manual**.
4. Para seleccionar la reubicación calendarizada en el nivel del pool, haga clic en **Relocation Schedule** para abrir el cuadro de diálogo **Manage Auto-Tiering**, como se muestra en la Figura 10.

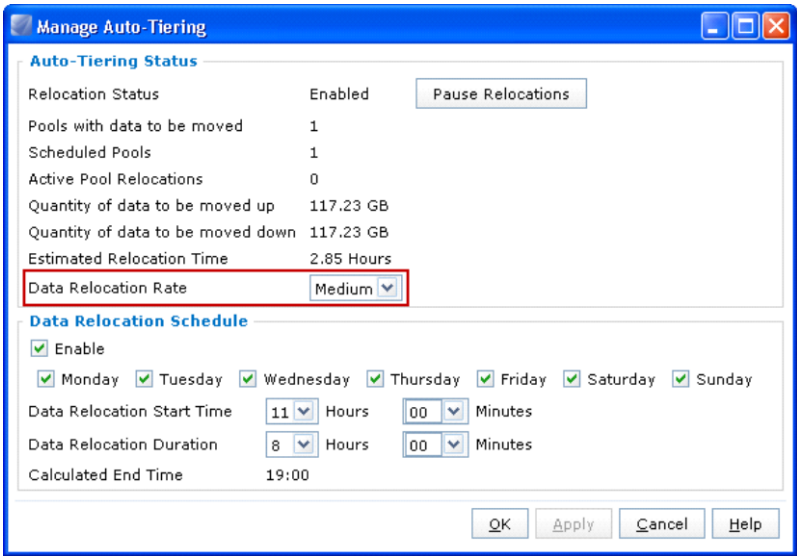


Figura 10. Cuadro de diálogo Manage Auto-Tiering

El valor de **Data Relocation Rate** está configurado en **Medium** para que los I/O del host no se vean afectados significativamente.

Nota: FAST VP es una herramienta completamente automatizada que permite calendarizar las reubicaciones para que se produzcan de manera automática. EMC recomienda que calendarice las reubicaciones en horarios de menor actividad para minimizar cualquier impacto potencial en el rendimiento.

Requisitos de la nube privada de VSPEX

Esta infraestructura comprobada de cómputo del usuario final de VSPEX requiere múltiples servidores de aplicaciones. A menos que se especifique lo contrario, todos los servidores utilizan Microsoft Windows Server 2012 R2 como el SO base. La Tabla 12 enumera los requisitos mínimos para cada servidor de infraestructura requerido.

Tabla 12. Requisitos mínimos del servidor de la infraestructura

Servidor	CPU	RAM (GB)	IOPS	Capacidad de almacenamiento (GB)
Controladores de dominio (cada uno)	2 CPU virtuales	4	25	32
SQL Server	2 CPU virtuales	6	100	200
vCenter Server	4 CPU virtuales	8	100	80
Controladores de View (cada uno)	4 CPU virtuales	12	50	32

Los siguientes documentos describen los requisitos de los componentes opcionales de vRealize Operations Manager for Horizon View y VMware Workspace, respectivamente:

- *Perfil de la plataforma VMware vRealize Operations Manager for Horizon View*
- *EMC VSPEX for VMware Horizon Workspace: guía de la solución*

Diseño del almacenamiento de la nube privada

Esta solución requiere los siguientes volúmenes del tamaño indicado para almacenar las máquinas virtuales señaladas:

- Un volumen de 1 TB para alojar las máquinas virtuales de la infraestructura, que pueden incluir vCenter Server, View Connection Server, Active Directory Server y Microsoft SQL Server
- Para configuraciones de un máximo de 1,750 escritorios, un volumen de 1.8 TB para alojar las bases de datos y máquinas virtuales de vRealize Operations Manager for Horizon View
- Para configuraciones de un máximo de 3,500 escritorios, un volumen de 3.6 TB para alojar las bases de datos y máquinas virtuales de vRealize Operations Manager for Horizon View

Para obtener información sobre configuraciones de mayor tamaño, comuníquese con su representante de ventas de EMC.

Configurar controladores de eventos de XtremIO

Puede configurar XtremIO para enviar alertas por correo electrónico cuando se produzcan eventos de cluster menores, como por ejemplo, los eventos relacionados con la capacidad sin clusters. La *Guía del usuario del arreglo de almacenamiento EMC XtremIO* proporciona una lista completa de las alertas y errores de XtremIO.

Para crear un controlador de eventos que envíe una alerta por correo electrónico cuando se produzcan estos eventos, siga los pasos a continuación:

1. En XtremIO Storage Management Application, seleccione **Alerts & Events** de la barra de menú.
2. En la ventana **Alerts & Events**, haga clic en **Events**.
3. Haga clic en el ícono **Display Event Handlers**, como se muestra en la Figura 11.

Figura 11. Opción Display Event Handlers de XtremIO

4. En la ventana **Event Handlers**, haga clic en **Add**.
5. En el cuadro de diálogo **Add Event Handler**, seleccione lo siguiente, donde "cluster" corresponde al nombre del cluster de XtremIO según lo especificado durante la instalación, como se muestra en la Figura 12:
   - **Category**: Software
   - **Severity**: Menor
   - **Entity**: Cluster
   - **Entity Details**: Nombre del cluster
6. En el mismo cuadro de diálogo, seleccione **Send e-mail** y luego haga clic en **OK**.

   También puede configurar la alerta seleccionando **Send SNMP Trap** o **Send to Syslog**.

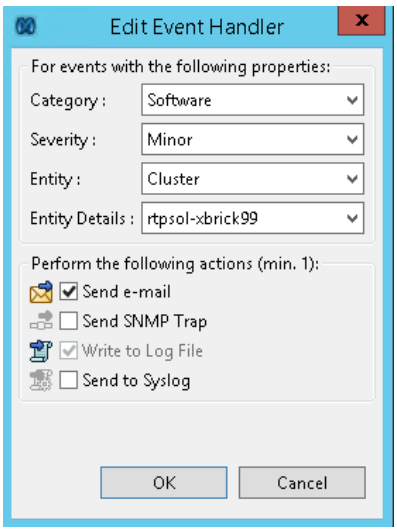


Figura 12. Cuadro de diálogo Edit Event Handler en XtremIO

7. **Seleccione** Administration en la barra de menú.
8. En **Administration** - **Email Configuration**, haga clic en Add para agregar cualquier dirección de correo electrónico que deba recibir copias de alertas de XtremIO.

   Si configuró el controlador de eventos para que use SNMP o Syslog para enviar alertas, configure esas opciones en **SNMP Configuration** o **Syslog Configuration**, según corresponda.

Instalación y configuración de los hosts vSphere

En esta sección se proporciona información sobre la instalación y la configuración de los hosts vSphere y los servidores de infraestructura necesarios para que sean compatibles con la arquitectura. En la Tabla 13 se describen las tareas que se deben realizar.

Tabla 13. Tareas para la instalación de servidores

Tarea	Descripción	Referencia
Instalar vSphere	Instale el hipervisor vSphere en los servidores físicos implementados para la solución.	*VMware vSphere Installation and Setup Guide*
Configurar la red vSphere	Configure la red vSphere, incluido el trunking de la tarjeta de interfaz de red (NIC), los puertos VMkernel y los grupos de puertos de máquinas virtuales.	• Documentación de VMware vSphere Networking • Configurar la red vSphere
Agregar hosts vSphere a los grupos de iniciadores de XtremIO	Agregar hosts vSphere a los grupos de iniciadores creados en Preparación y configuración de los arreglos de almacenamient.	*VMware vSphere Installation and Setup Guide*
Conectar áreas de almacenamiento de datos de VMware	Conecte las áreas de almacenamiento de datos de VMware a los hosts vSphere implementados para la solución.	• *vSphere Storage Guide* • Conectar áreas de almacenamiento de datos de vSphere
Optimizar vSphere	Realice los cambios de configuración necesarios para garantizar el rendimiento óptimo del arreglo XtremIO.	• *Guía del usuario del arreglo de almacenamiento EMC XtremIO* • Optimizar vSphere para XtremIO

Instalar vSphere

Cuando encienda los servidores en uso para vSphere, confirme o active la configuración de virtualización de CPU asistida por hardware y la configuración de la virtualización de MMU asistida por hardware en el BIOS de cada servidor. Si los servidores cuentan con un controlador RAID, EMC recomienda configurar el espejeado en los discos locales.

Utilice los medios de instalación de vSphere para instalar el hipervisor en cada uno de los servidores. Para la instalación, se requieren los nombres de host vSphere, las direcciones IP y una contraseña raíz. La Hoja de trabajo de configuración del cliente proporciona los valores adecuados.

Configurar la red vSphere

En la guía de VMware vSphere Networking se describe la configuración de red de vSphere, incluido el balanceo de carga, la agregación de vínculos y las opciones de failover. Elija la opción de balanceo de carga apropiada de acuerdo con lo que es compatible con la infraestructura de red. Para obtener mayor información, consulte la lista de documentos en el Documentación de referencia.

Tarjetas de interfaz de red

Durante la instalación de vSphere, se crea un switch virtual estándar (vSwitch). De forma predeterminada, vSphere elige solo una NIC física como un vínculo superior de vSwitch. Para mantener los requisitos de redundancia y ancho de banda, configure una NIC adicional usando la consola vSphere o estableciendo conexión con el host vSphere desde el cliente vSphere.

Cada servidor vSphere debe tener múltiples tarjetas NIC para cada red virtual con el fin de asegurar la redundancia y permitir el balanceo de carga de la red, la agregación de vínculos y el failover del adaptador de red.

Puertos VMkernel

Cree puertos VMkernel según sea necesario de acuerdo con la configuración de la infraestructura:

- Puerto VMkernel para vMotion
- Grupos de puerto de escritorios virtuales (utilizados por los equipos de escritorio virtuales para comunicarse en la red)

La g*uía de VMware vSphere Networking* describe el procedimiento para establecer estas configuraciones. Para mayor información, consulte la lista de documentos en Documentación de referencia.

Conectar áreas de almacenamiento de datos de vSphere

Conecte las áreas de almacenamiento de datos configuradas en Preparación y configuración de los arreglos de almacenamiento a los servidores vSphere apropiados. Estas incluyen las áreas de almacenamiento de datos configuradas para:

- Almacenamiento de escritorios virtuales
- Almacenamiento de máquinas virtuales de la infraestructura (si se requiere)
- Almacenamiento de SQL Server (si se requiere)

Para permitir que los servidores vSphere tengan acceso a los volúmenes de XtremIO, configure los grupos de iniciadores de XtremIO y agregue los hosts de vSphere correspondientes a cada uno de la siguiente manera:

1. En XtremIO Storage Management Application, seleccione **Configuration**.
2. En **Initiator Group**, haga clic en **Add**.
3. En el cuadro de diálogo **Add New Initiator Group**, escriba un nombre en el campo **Initiator Group Name** y, a continuación, haga clic en **Add**.
4. En el cuadro de diálogo **Add Initiator**, escriba un nombre en el campo **Initiator Name** y, a continuación, use el cuadro de lista **Initiator Port Address** para seleccionar el puerto de iniciador de un servidor vSphere que se debe encontrar en el grupo de iniciadores de destino.
5. Haga clic en **OK** para volver al cuadro de diálogo **Add Initiator**.
6. Repita los pasos 4 y 5 según sea necesario para agregar todos los puertos de iniciador al grupo de iniciadores. Una vez que haya agregado todos los iniciadores, haga clic en Finish.
7. En **Configuration**, seleccione los volúmenes de destino en **Volumes**, seleccione el grupo de iniciadores de destino en **Initiator Groups**, haga clic en **Map All** y, a continuación, haga clic en **Apply** para completar el proceso y brindarles a los servidores vSphere acceso a los volúmenes seleccionados.
8. Repita el paso anterior según sea necesario para otorgar al resto de los grupos de iniciadores acceso a los volúmenes restantes.
9. Ejecute la operación **Rescan for Datastores** en los hosts de vSphere de modo que estos tengan acceso inmediato a los volúmenes de XtremIO a los que se les otorgó acceso.
10. Repita este procedimiento según sea necesario, creando un grupo de iniciadores para cada cluster de vSphere.

La *Guía de almacenamiento de VMware vSphere* proporciona instrucciones sobre cómo dar formato a las áreas de almacenamiento de datos de vSphere una vez configurados los grupos de iniciadores de XtremIO. Para obtener mayor información, consulte la lista de documentos en el Documentación de referencia.

Optimizar vSphere para XtremIO

Debe realizar varios cambios en la configuración de vSphere para garantizar el rendimiento óptimo del arreglo XtremIO cuando se utiliza con vSphere.

Nota: Las configuraciones que se describen en esta sección se aplican solo a los hosts de vSphere conectados con los arreglos XtremIO; no se deben aplicar a las áreas de almacenamiento de datos de bloques alojadas en otros arreglos, incluidos otros arreglos de EMC. Puede utilizar estas configuraciones en los hosts de vSphere conectados a las áreas de almacenamiento de datos NFS y XtremIO. Estas configuraciones no afectarán la comunicación con esas áreas de almacenamiento de datos NFS.

Entre los cambios requeridos, los cuales se describen en la *Guía del usuario del arreglo de almacenamiento de EMC XtremIO*, se incluyen los siguientes:

- Cambiar la configuración de selección de ruta del dispositivo de almacenamiento de vSphere a **Round Robin (VMware)** para cada área de almacenamiento de datos de vSphere. Puede realizar esta modificación mediante el siguiente comando vSphere PowerCLI para cada cluster, reemplazando *cluster* por el nombre del cluster de vSphere donde residen los hosts de vSphere de destino:

  ```
  Get-VMHost -location cluster | get-scsilun -luntype "disk"
  | where {$_.MultipathPolicy -ne "RoundRobin"} | Set-ScsiLun
  -MultipathPolicy "RoundRobin"
  ```

- Cambie la configuración de vSphere **Disk.SchedQuantum** a **64** y la configuración **Disk.DiskMaxIOSize** a **4,096**. Puede realizar estos cambios mediante los siguientes comandos vSphere PowerCLI para cada cluster, reemplazando *cluster* por el nombre del cluster de vSphere donde residen los hosts de vSphere de destino:

  ```
  Get-VMhost -location cluster | Set-
  VMhostAdvancedConfiguration Disk.SchedQuantum -Value 64
  Get-VMhost -location cluster | Set-
  VMhostAdvancedConfiguration Disk.DiskMaxIOSize -Value 4096
  ```

- Cambie la configuración de vSphere **Disk.SchedNumReqOutstanding** a **256** para cada área de almacenamiento de datos de vSphere. Puede realizar esta modificación mediante el siguiente script vSphere PowerCLI para cada cluster, reemplazando *ClusterName* por el nombre del cluster de destino:

  ```
  $vmhosts = get-vmhost –location ClusterName
  foreach ($vmhost in $vmhosts) {
  $esxcli = get-esxcli -vmhost $vmhost
  $AllLUNs = get-scsilun -vmhost $vmhost | where {$_.vendor -
  eq "XtremIO"}
  foreach ($lun in $AllLUNs) {
  $CN = $lun.canonicalname
  $EsxCli.storage.core.device.set($null, $cn, $null, $null,
  $null, $null, $null, 256, $on)
  }
  }
  ```

Implementación de EMC Virtual Storage Integrator

El plug-in EMC Virtual Storage Integrator (VSI) permite a los administradores realizar la mayoría de las tareas administrativas comunes de XtremIO desde vSphere Web Client en lugar de tener que utilizar la consola de administración de XtremIO. Además, los administradores pueden usar el plug-in para efectuar optimizaciones clave del host de vSphere para XtremIO, en lugar de tener que utilizar vSphere PowerCLI. Si un arreglo VNX se implementa como parte de esta solución, los administradores pueden usar el plug-in VSI para administrar también el almacenamiento VNX.

Si su solución utiliza el plug-in VSI, consulte *EMC VSI para VMware vSphere Web Client: guía del producto* para recibir instrucciones sobre la instalación, configuración y funcionamiento.

En la Figura 13 se muestra una instalación de EMC VSI que se integró a vSphere Web Client, como se visualiza en la página de inicio de vCenter.

Figura 13. vSphere Web Client: Integración con EMC VSI

La opción **vCenter Home** › **Storage Systems** enumera todos los sistemas de almacenamiento de EMC tras haberlos agregado al plug-in VSI. En el ejemplo de la Figura 14, el arreglo XtremIO se agregó y está disponible para su administración en vSphere Web Client.

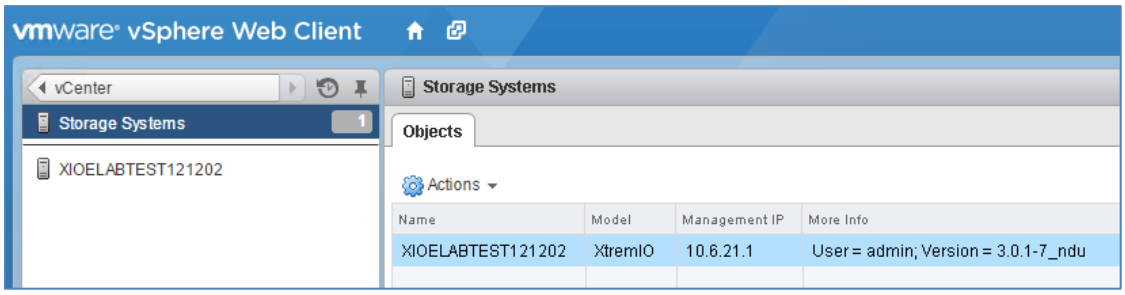


Figura 14. vSphere Web Client: EMC VSI: sistemas de almacenamiento

Una vez que haya agregado un arreglo al plug-in VSI, vSphere Web Client muestra todas las áreas de almacenamiento de datos del arreglo en una lista. Haga clic con el botón secundario en un área de almacenamiento de datos y seleccione **All EMC VSI Plugin Actions** para acceder a todas las acciones que puede aplicar a dicha área de almacenamiento, como se indica en la Figura 15.

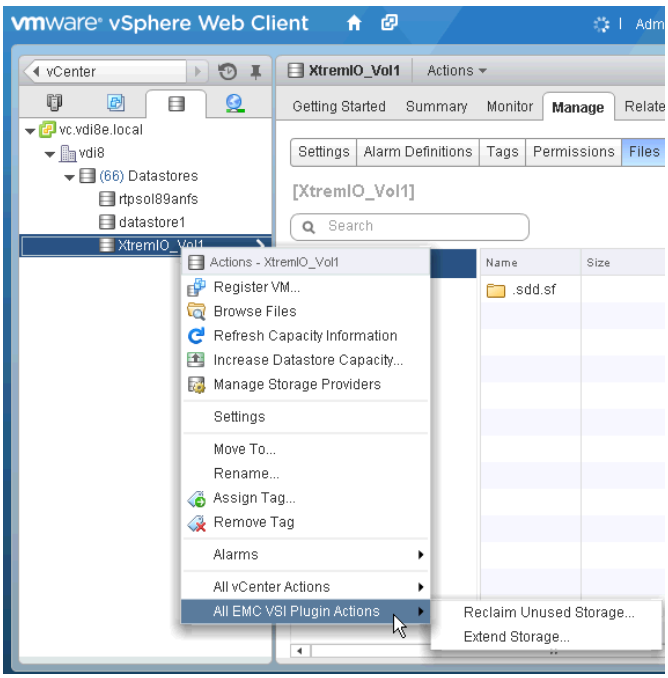


Figura 15. vSphere Web Client: acciones del área de almacenamiento de datos de EMC VSI para XtremIO

Optimización de hosts de vSphere para XtremIO

Debe actualizar varias configuraciones de hosts de vSphere para garantizar el rendimiento óptimo del arreglo XtremIO con vSphere. La *guía del usuario del arreglo de almacenamiento EMC XtremIO* describe estas configuraciones.

Es posible utilizar cualquiera de los siguientes elementos para implementar las configuraciones requeridas:

- Plug-in de EMC VSI
- Scripts vSphere PowerCLI

Ambas opciones producen los mismos resultados. Sin embargo, el plug-in de EMC VSI ofrece la forma más rápida y sencilla de implementar las configuraciones requeridas. Los scripts PowerCLI automatizan el proceso y son útiles en ambientes donde se prefiere específicamente la implementación automatizada de las configuraciones.

Si los volúmenes de XtremIO ya se presentaron a los hosts de vSphere, debe usar el plug-in de EMC VSI en vez de los scripts PowerCLI para implementar las configuraciones.

Nota: Las configuraciones se aplican solamente a los hosts de vSphere conectados a los arreglos XtremIO. No las aplique a áreas de almacenamiento de datos en bloques alojadas en otros tipos de arreglos, incluidos otros arreglos de EMC. Sin embargo, puede aplicar estas configuraciones a los hosts de vSphere conectados a las áreas de almacenamiento de datos NFS, ya que las configuraciones no afectarán la comunicación con dichas áreas de almacenamiento de datos NFS.

Uso del plug-in de EMC VSI para optimizar el rendimiento de vSphere y XtremIO

Para configurar la optimización con el plug-in de EMC VSI, siga los pasos a continuación:

1. Inicie sesión en vSphere Web Client con una cuenta que tenga permisos administrativos para vSphere y el plug-in de EMC VSI.
2. Navegue hasta la ventana **Hosts and Clusters**.
3. En la lista de hosts de vSphere, haga clic con el botón secundario en un host que requiera la configuración actualizada y seleccione **All EMC VSI Plugin Actions** › **ESX Host Settings**, como se muestra en la Figura 16.

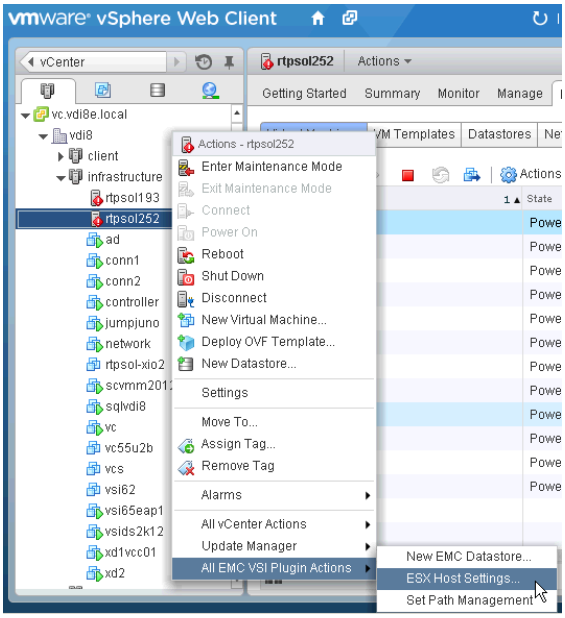


Figura 16. vSphere Web Client: configuración del host de EMC VSI

4. En **Set Host Settings**, seleccione todas las opciones disponibles, como se muestra en la Figura 17, y haga clic en **Next**.

Nota: Se requiere acceso de protocolo Secure Shell (SSH) al host de vSphere y es necesario reiniciar el sistema para implementar todas las configuraciones.

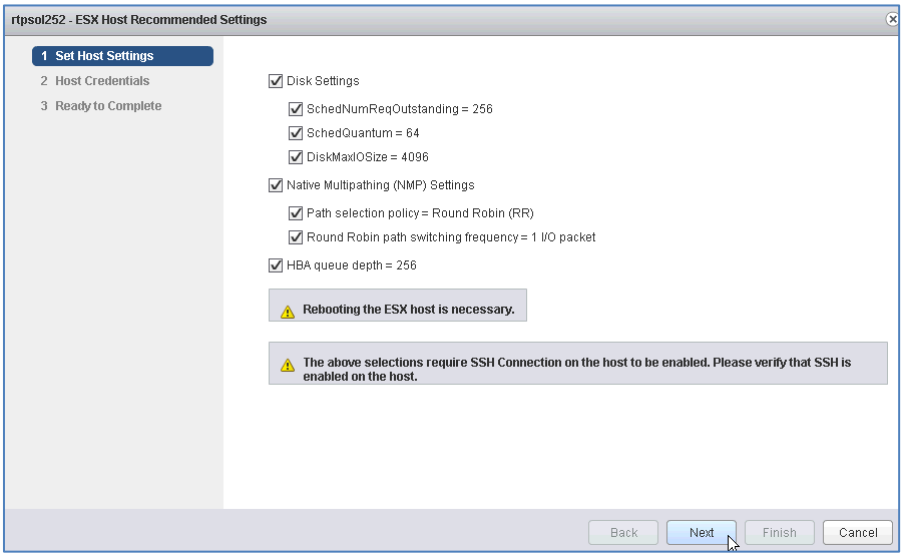

rtpsol252 - ESX Host Recommended Settings
1 Set Host Settings
2 Host Credentials
3 Ready to Complete
Disk Settings
SchedNumReqOutstanding = 256
SchedQuantum = 64
DiskMaxIOSize = 4096
Native Multipathing (NMP) Settings
Path selection policy = Round Robin (RR)
Round Robin path switching frequency = 1 I/O packet
HBA queue depth = 256
Rebooting the ESX host is necessary.
The above selections require SSH Connection on the host to be enabled. Please verify that SSH is enabled on the host.
Back
Next
Finish
Cancel

Figura 17. vSphere Web Client: configuración del host de EMC VSI

5. En **Host Credentials**, escriba las credenciales de una cuenta local en el host de vSphere y haga clic en Next.

   Nota: La cuenta local debe tener acceso raíz.

6. En **Ready to Complete**, revise los cambios propuestos y, a continuación, haga clic en Finish.
7. Repita los pasos del tres al seis para los demás hosts de vSphere en el cluster.

Los hosts de vSphere ahora cuentan con la configuración óptima para su uso con XtremIO.

Instalación y configuración de la base de datos de SQL Server

Tabla 14 describe cómo instalar y configurar una base de datos Microsoft SQL Server para la solución. Una vez finalizadas las tareas, SQL Server se configura en una máquina virtual, con todas las bases de datos requeridas por vCenter, VMware vSphere Update Manager, Horizon View y View Composer configuradas para su uso.

Nota: EMC recomienda poner el volumen del SO de la máquina virtual de SQL Server en un pool de nube privada de VSPEX. La Tabla 12, en la página 38, proporciona los valores recomendados de CPU y memoria.

Tabla 14. Tareas para la configuración de una base de datos de SQL Server

Tarea	Descripción	Referencia
Crear una máquina virtual para Microsoft SQL Server	Cree la máquina virtual para alojar el SQL Server en uno de los servidores vSphere designados para las máquinas virtuales de la infraestructura, y use el área de almacenamiento de datos designada para la infraestructura compartida. Verifique que el servidor virtual cumpla con los requisitos de hardware y software.	*VMware vSphere Virtual Machine Administration Guide*
Instalar Microsoft Windows en la máquina virtual	Instale Microsoft Windows Server 2012 R2 Standard Edition en la máquina virtual.	Instalar e implementar Windows Server 2012 R2
Instalar Microsoft SQL Server	Instale Microsoft SQL Server 2012 en la máquina virtual.	Instalación de SQL Server (SQL Server 2012)
Configurar la base de datos para vCenter Server	Cree la base de datos requerida para vCenter Server en el área de almacenamiento de datos correspondiente.	*Preparing vCenter Server Databases*
Configurar la base de datos para vSphere Update Manager	Cree la base de datos requerida para vSphere Update Manager en el área de almacenamiento de datos apropiada.	*Preparing the Update Manager Database*
Configurar la base de datos para View Composer	Cree la base de datos requerida para View Composer en el área de almacenamiento de datos apropiada.	*VMware Horizon View Installation Guide*
Configurar la base de datos de View Manager	Cree la base de datos requerida para los registros de eventos de View Manager en el área de almacenamiento de datos apropiada.	
Configurar los permisos de las bases de datos de Horizon View y View Composer	Configure el servidor de base de datos con los permisos apropiados para las bases de datos de Horizon View y View Composer.	*VMware Horizon View Installation Guide*
Configurar los permisos de la base de datos de vCenter	Configure el servidor de base de datos con los permisos apropiados para vCenter.	*Preparing vCenter Server Databases*
Configurar los permisos de la base de datos de vSphere Update Manager	Configure el servidor de base de datos con los permisos apropiados para vSphere Update Manager.	*Preparing the Update Manager Database*

Implementación de VMware vCenter Server

En la Tabla 15 se describen las tareas que se deben realizar para configurar VMware vCenter Server para la solución.

Nota: EMC recomienda poner el volumen del sistema operativo de la máquina virtual de vCenter Server en el pool de nube privada de VSPEX. La Tabla 12, en la página 38, proporciona los valores recomendados de CPU y memoria.

Tabla 15. Tareas para la configuración de vCenter

Tarea	Descripción	Referencia
Crear la máquina virtual del host vCenter	Crear una máquina virtual para vCenter Server.	*VMware vSphere Virtual Machine Administration Guide*
Instalar el SO huésped de vCenter	Instale Windows Server 2012 R2 Standard Edition en la máquina virtual del host de vCenter.	Documentación de vSphere
Actualizar la máquina virtual	Instale las herramientas de VMware y active la aceleración de hardware y el acceso a la consola remota.	*vSphere Virtual Machine Administration Guide*
Crear las conexiones ODBC de vSphere Update Manager	Cree las conexiones ODBC de vSphere Update Manager de 32 y 64 bits.	• *VMware vSphere Installation and Setup Guide* • *Installing and Administering VMware vSphere Update Manager*
Instalar vCenter Server	Instale el software vCenter Server.	*VMware vSphere Installation and Setup Guide*
Instalar vSphere Update Manager	Instale el software vSphere Update Manager.	*Instalación y administración de VMware vSphere Update Manager*
Crear un centro de datos virtual	Cree un centro de datos virtual.	*VMware vCenter Server and Host Management*
Aplicar números de licencia de vSphere	Escriba los números de licencia de vSphere en el menú de licencias de vCenter.	*VMware vSphere Installation and Setup*
Agregar hosts vSphere	Conecte vCenter Server a los hosts vSphere.	*VMware vCenter Server and Host Management Guide*
Configurar la agrupación en clusters de vSphere	Cree un cluster vSphere y traslade a él los hosts vSphere.	*VMware vSphere Resource Management Guide*
Instalar el plug-in vSphere Update Manager	Instale el plug-in vSphere Update Manager desde la consola de administración.	*Instalación y administración de VMware vSphere Update Manager*

Tarea	Descripción	Referencia
Implementar EMC PowerPath/VE	Use vSphere Update Manager para implementar el plug-in PowerPath/VE en todos los hosts vSphere.	*Guía de instalación y administración de EMC PowerPath/VE para VMware vSphere*
Instalar el plug-in EMC VSI para VMware vSphere	Instale el plug-in VSI para VMware vSphere en la consola de administración.	*EMC VSI para VMware vSphere: Administración de almacenamiento unificado: Guía del producto*
Instalar EMC PowerPath Viewer	Instale PowerPath Viewer en la consola de administración.	*Guía de instalación y de administración de EMC PowerPath Viewer*

Configurar View Connection Server

En esta sección se proporciona información sobre cómo instalar y configurar View Connection Server para la solución. Para una instalación nueva de Horizon View, VMware recomienda realizar las siguientes tareas en el orden que se muestra en la Tabla 16.

Nota: EMC recomienda poner el volumen del SO de las máquinas virtuales de View Connection Server en el pool de nube privada de VSPEX. La Tabla 12, en la página 38, proporciona los valores recomendados de CPU y memoria.

Tabla 16. Tareas para la configuración de View Connection Server

Tarea	Descripción	Referencia
Crear máquinas virtuales para View Connection Server	Cree dos máquinas virtuales en el cliente vSphere. Estas máquinas virtuales se usarán como hosts de View Connection Servers. Instalar Windows Server 2012 R2 como el SO huésped para los servidores.	*VMware Horizon View Installation Guide*
Instalar View Connection Server	Instale el software View Connection Server en una de las máquinas virtuales previamente preparadas. Ingrese el número de licencia de Horizon View en la consola del administrador de VMware View Manager.	Documentación de VMware Horizon View
Configurar la conexión de la base de datos de registros de eventos de Horizon View	Establezca la configuración de la base de datos de registros de eventos de Horizon View utilizando la información de la base de datos y las credenciales de inicio de sesión correspondientes.	
Agregar una réplica de la instancia de View Connection Server	Instale el software View Connection Server en el segundo servidor.	

Tarea	Descripción	Referencia
Configurar la conexión ODBC de View Composer	En vCenter Server o en un servidor Windows Server 2012 R2 dedicado, configure una conexión ODBC para la base de datos de View Composer previamente configurada.	
Instalar View Composer	Instale View Composer en el servidor utilizado en el paso anterior.	
Conectar Horizon View a vCenter y View Composer	Use la interfaz web de VMware View Manager para conectar Horizon View al servidor vCenter y View Composer.	*VMware Horizon View Administration Guide*
Preparar una máquina virtual maestra	Cree una máquina virtual maestra como la imagen base para los escritorios virtuales.	
Configurar políticas de grupo de View Persona Management	Configure políticas de grupo de Active Directory para activar View Persona Management.	
Configurar las políticas de grupo de redireccionamiento de carpetas para EMC Avamar	Configure las políticas de grupo de Active Directory para permitir el redireccionamiento de carpetas para Avamar.	
Configurar políticas de grupo de PCoIP de Horizon View	Configure las políticas de grupo de Active Directory para la configuración del protocolo PCoIP.	

Instalar View Connection Server

Instale el software Horizon View Connection Server de acuerdo con las instrucciones detalladas en la *VMware Horizon View Installation Guide*. Seleccione **Standard** cuando se le consulte por **View Connection Server**. Ingrese el número de licencia de Horizon View en la consola web de View Manager.

Configurar la conexión de la base de datos de registros de eventos de Horizon View

Configure la conexión de la base de datos de registro de eventos de Horizon View utilizando el nombre del servidor de la base de datos, el nombre de la base de datos y las credenciales de inicio de sesión de la base de datos. Consulte la *VMware Horizon View Installation Guide* para obtener instrucciones específicas sobre cómo configurar el registro de eventos.

Agregar una réplica de la instancia de View Connection Server

Repita el proceso de instalación de View Connection Server en la segunda máquina virtual de destino. Cuando se le consulte por el tipo de servidor de la conexión, especifique **Replica** y proporcione las credenciales de administrador de Horizon View para replicar los datos de configuración de Horizon View de la primera instancia de View Connection Server.

Configurar la conexión ODBC de View Composer

En el servidor que alojará el servicio View Composer, cree una conexión ODBC para la base de datos de View Composer previamente configurada. Consulte la *VMware Horizon View Installation Guide* para obtener instrucciones específicas sobre cómo configurar la conexión ODBC.

Instalar View Composer

En el servidor que alojará el servicio View Composer, instale el software View Composer. Especifique la conexión ODBC previamente configurada cuando se le solicite durante el proceso de instalación. Consulte la *VMware Horizon View Installation Guide* para obtener instrucciones específicas sobre cómo configurar la conexión ODBC.

Conectar Horizon View a vCenter y View Composer

En la consola web de VMware View Manager, cree la conexión entre Horizon View y vCenter Server y View Composer. Consulte la *VMware Horizon View Administration Guide* para obtener instrucciones específicas sobre cómo crear las conexiones. Cuando se le presente la opción de activar el almacenamiento en caché de hosts de vSphere (también conocido como Horizon View Storage Accelerator o caché de lectura basada en contenido), active la opción y establezca el tamaño de la caché en 2 GB, la capacidad máxima compatible.

También puede activar la opción de **espacio en disco Reclaim VM**. Si activa la opción de **espacio en disco Reclaim VM**, debe especificar un período sin disponibilidad que controle cuándo no se debe procesar la operación. Dado que la operación no se debe ejecutar durante períodos de uso intensivo, incluya esos momentos en el período sin disponibilidad. De forma predeterminada, la recuperación de espacio solo se ejecutará cuando haya que recuperar 1 GB de espacio o más. Se puede especificar otro valor al implementar los pools de escritorios.

Preparar una máquina virtual maestra

Para preparar la máquina virtual maestra:

1. En vSphere Web Client, cree una máquina virtual con la especificación de hardware VMware, versión 9.

   No se pueden crear máquinas virtuales de versión 9 con vSphere Client; se debe usar vSphere Web Client.

2. Instale el SO huésped Windows 7 o Windows 8.1.
3. Instale las herramientas de integración apropiadas, tales como las herramientas de VMware.
4. Optimice las configuraciones del sistema operativo para evitar servicios en segundo plano innecesarios que generen operaciones de I/O extrañas y perjudiquen el rendimiento general del arreglo de almacenamiento.

   Para obtener información detallada, consulte la *guía de optimización de VMware Horizon View para Windows 7 y 8*.

5. Instale las herramientas o aplicaciones de otros fabricantes pertinentes al ambiente, tales como Microsoft Office.
6. Instale el software del cliente Avamar para escritorio/laptop.
7. Para obtener información detallada, consulte *EMC Backup and Recovery for VSPEX for End-User Computing with VMware Horizon View: guía de diseño e implementación*.
8. Instale el agente Horizon View.

   Nota: Si utiliza la función View Persona Management, instale el componente de Persona Management del agente Horizon View en este momento. Asegúrese de que la opción Persona Management esté seleccionada durante la instalación del agente de Horizon View.

9. Instale el agente de VMware Workspace (opcional; solo se requiere si se accede a VMware Workspace desde los escritorios de Horizon View).
10. Si está implementando escritorios de clonación completa, cree una especificación de personalización de vSphere que se usará para la personalización de escritorios.

    Consulte el documento de VMware *vSphere Virtual Machine Administration Guide* para obtener información sobre cómo crear y administrar especificaciones de personalización. Este paso no es necesario si implementa escritorios de clonación vinculada.

Configurar políticas de grupo de Horizon View Persona Management

View Persona Management se activa mediante políticas de grupo de Active Directory que se aplican a la unidad organizacional (OU) que contiene las cuentas de computadoras de escritorio virtuales. Las plantillas de política de grupo de View se encuentran en el directorio **\Program Files\VMware\VMware Horizon View\Server\extras\GroupPolicyFiles** de View Connection Server.

Configurar las políticas de grupo de redireccionamiento de carpetas para EMC Avamar

Active el redireccionamiento de carpetas mediante políticas de grupo de Active Directory que se aplican a la unidad organizacional (OU) que contiene las cuentas de usuario de escritorios virtuales. El redireccionamiento de carpetas de Active Directory se usa (en lugar del redireccionamiento de carpetas de View Persona Management) para verificar que las carpetas mantengan las consistencias de asignación de nombres que requiere el software Avamar. Para obtener información detallada, consulte *EMC Backup and Recovery for VSPEX for End User Computing for VMware Horizon View*.

Configurar políticas de grupo de PCoIP de Horizon View

La configuración del protocolo PCoIP de Horizon View se controla mediante políticas de grupo de Active Directory que se aplican a la OU que contiene los servidores de Horizon View Connection Server. Las plantillas de políticas de grupo de Horizon View se encuentran en el directorio **\Program Files\VMware\VMware View\Server\extras\GroupPolicyFiles** de Horizon View Connection Server. Se debe usar la plantilla de políticas de grupo **pcoip.adm** para especificar la siguiente configuración del protocolo PCoIP:

- **Maximum Initial Image Quality Value**: 70
- **Maximum Frame Rate Value**: 24
- **Apague Build-to-Lossless:** Activado

Nota: Las velocidades de frames de sesión PCoIP y las calidades de imágenes más altas pueden afectar adversamente los recursos del servidor.

Provisionar escritorios virtuales con View Composer

Use la consola del administrador de View Manager para implementar los escritorios virtuales de la siguiente manera:

1. Cree un **Automated Desktop Pool**.
2. Especifique el método recomendado para **User Assignment**:
   - **Dedicated**: Los usuarios reciben el mismo escritorio cada vez que inician sesión en el pool. Este método se usa generalmente con escritorios de clonación completa.

- **Floating**: Los usuarios reciben escritorios elegidos al azar desde el pool cada vez que inician sesión.

3. Haga clic en **Next**.
4. Especifique los valores en **View Composer linked clones** o en **Full virtual machines** (clones completos) y haga clic en **Next**.
5. Determine el valor correspondiente al **ID** del pool de escritorios y haga clic en **Next**.
6. Configure los valores de **Desktop Pool Settings** según corresponda y haga clic en **Next**.
7. Configure los valores de **Provisioning Settings** según corresponda y haga clic en **Next**.
8. Si está creando un pool de clones vinculados, acepte los valores predeterminados para **View Composer Disks** o edite los valores según sea necesario.

   Este paso no se muestra al crear un pool de máquinas virtuales completas.
9. Si se usa **View Persona Management**, seleccione **Do not redirect Windows profile** en la sección **Persistent Disk**, como se muestra en la Figura 18.

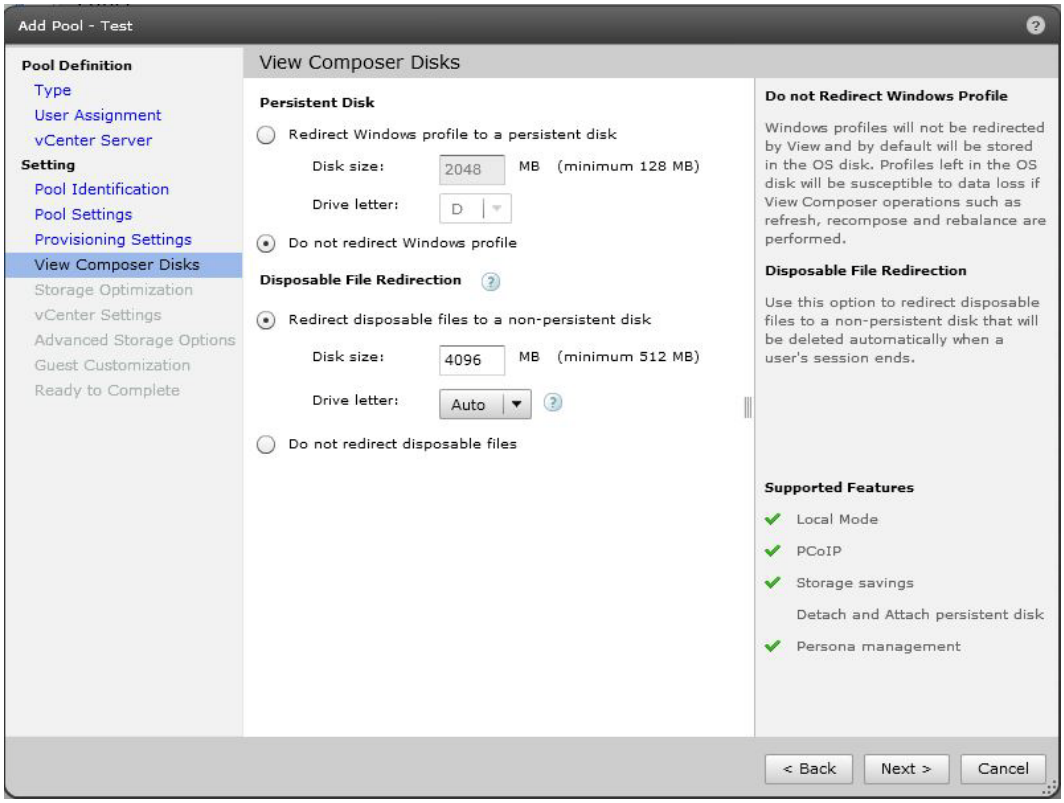

Add Pool - Test
Pool Definition
Type
User Assignment
vCenter Server
Setting
Pool Identification
Pool Settings
Provisioning Settings
View Composer Disks
Storage Optimization
vCenter Settings
Advanced Storage Options
Guest Customization
Ready to Complete
View Composer Disks
Persistent Disk
Redirect Windows profile to a persistent disk
Disk size: 2048 MB (minimum 128 MB)
Drive letter: D
Do not redirect Windows profile
Disposable File Redirection
Redirect disposable files to a non-persistent disk
Disk size: 4096 MB (minimum 512 MB)
Drive letter: Auto
Do not redirect disposable files
Do not Redirect Windows Profile
Windows profiles will not be redirected by View and by default will be stored in the OS disk. Profiles left in the OS disk will be susceptible to data loss if View Composer operations such as refresh, recompose and rebalance are performed.
Disposable File Redirection
Use this option to redirect disposable files to a non-persistent disk that will be deleted automatically when a user's session ends.
Supported Features
Local Mode
PCoIP
Storage savings
Detach and Attach persistent disk
Persona management
< Back
Next >
Cancel

Figura 18. Cuadro de diálogo de View Composer Disks

10. Haga clic en **Next**.

    Aparecerá el cuadro de diálogo **Storage Optimization**. No se requieren cambios.
11. Haga clic en **Next**.

12. Si está implementando un pool de clones vinculados de View Composer, seleccione la máquina virtual principal, el snapshot de la máquina virtual, la carpeta, los hosts o clusters de vSphere, el pool de recursos de vSphere y las áreas de almacenamiento de datos correspondientes.

    Si está configurando un pool de máquinas virtuales completas, seleccione la plantilla de máquina virtual, la carpeta, el host o cluster de vSphere, el pool de recursos de vSphere y las áreas de almacenamiento de datos correspondientes.

13. Haga clic en **Next**.

14. De manera opcional, active **Use View Storage Accelerator** para el pool de escritorios y especifique los horarios sin disponibilidad de regeneración de la caché.

    Si está implementando un pool de clones vinculados de View Composer, también puede activar la opción **Reclaim VM disk space** y especificar los horarios sin disponibilidad en **Blackout Times**.

15. Especifique las opciones de personalización de imágenes según corresponda, seleccionando **Use QuickPrep** para pools de clones vinculados de View Composer o **Use a customization specification (Sysprep)** para pools de máquinas virtuales completas (clones completos).

16. Complete el proceso de creación del pool para iniciar la creación del pool de escritorios virtuales.

17. En caso de que se utilice View Persona Management, configúrelo siguiendo las instrucciones proporcionadas en *Horizon View Installation Guide*.

Provisionar escritorios virtuales con VSI

Use EMC Virtual Storage Integrator (VSI) para VMware vSphere Web Client para implementar escritorios virtuales de clonación completa y agréguelos a un pool nuevo de la siguiente manera:

Nota: También es posible provisionar los escritorios virtuales a un pool existente. Para obtener información sobre cómo provisionar escritorios virtuales a un pool existente y sobre cómo configurar el ambiente VSI, consulte *EMC VSI para VMware vSphere Web Client: guía del producto.*

---

1. Inicie sesión en VMware vSphere Web Client.

2. Haga clic con el botón secundario en la máquina virtual de la imagen principal y seleccione **All EMC VSI Plugin Actions › EMC Clone**.

3. En el campo **Select base name and folder**, ingrese un nombre para el clon, seleccione la carpeta de destino y, a continuación, haga clic en Next.

4. En el cuadro de lista **Select a compute resource**, seleccione un cluster, host, vApp o pool de recursos para ejecutar los clones de máquinas virtuales; luego, haga clic en Next.

5. En las opciones de Select clone, proporcione la siguiente información:

   - **Clone count**: ingrese la cantidad de clones que desea crear.

- **Generated clone name**:
  - **Add leading zeros to index used to generate names**: seleccione esta opción para agregar ceros iniciales a los números de índice en los nombres de archivo.
  - **Number of digits in index**: especifique la cantidad total de dígitos que se anexarán al final del nombre de los clones.
- **Customization specification**: muestra en una lista todas las definiciones personalizadas desde el administrador de especificaciones de personalización.
- **Select destination datastore**: seleccione un área de almacenamiento de datos de XtremIO existente o seleccione New para crear una nueva área de almacenamiento de datos de destino para los clones.
- **Power on virtual machines after creation**: seleccione esta opción para encender automáticamente el clon de máquina virtual.

6. En **Connection Broker Information**, seleccione **Integrate with VMware View** y haga clic en **Next**.
7. En **Pool Choice**, seleccione un VMware View Server de la lista, seleccione **Add VMs to a new Pool** y haga clic en Next.
8. En **Pool Name**, ingrese un ID único, un nombre para visualizar y una descripción opcional en las casillas correspondientes; luego, seleccione una opción para **Desktop Persistence**.
9. **En Pool Settings**, seleccione los valores adecuados para las siguientes opciones:
   - **Cuando la máquina virtual no está en uso**
   - **Cierre de sesión automático después de desconectar**
   - **Permitir que los usuarios reinicien su escritorio**
   - **Protocolo de visualización predeterminado**
   - **Calidad de Adobe Flash**
   - **Regulación de Adobe Flash**
10. En la ventana **Ready to Complete**, revise los elementos que seleccionó y, a continuación, haga clic en **Finish**.

Recuperación del espacio de la capacidad física de XtremIO

vSphere no marca los bloques como disponibles de manera automática después de que se borra su contenido. Para devolver espacio sin utilizar al arreglo XtremIO para usarlo en el futuro, debe ejecutar una operación SCSI UNMAP por cada área de almacenamiento de datos de vSphere desde la ventana de mantenimiento del centro de datos.

Es posible realizar una operación SCSI UNMAP mediante cualquiera de los métodos siguientes:

- Use un script para ejecutar el comando **esxcli storage vmfs unmap** en cualquiera de los hosts vSphere conectados al área de almacenamiento de datos de destino. El comando está disponible a partir de la versión 5.5 de vSphere y es ideal para ambientes donde se recomienda automatizar el proceso SCSI UNMAP.

- Use el plug-in de EMC VSI para llevar a cabo la operación rápidamente en vSphere Web Client. Este método requiere que el plug-in de EMC VSI esté instalado y configurado en el ambiente vSphere y que esté asociado con el arreglo XtremIO de destino.

Ambos métodos producen el mismo resultado, por lo que debe seleccionar el método que se ajuste mejor a su régimen de mantenimiento de vSphere. Para obtener más información acerca de la operación SCSI UNMAP, consulte el artículo *Using esxcli in vSphere 5.5 to reclaim VMFS deleted blocks on thin-provisioned LUNs (2057513)* en la base de conocimientos de VMware.

Consideraciones de la operación SCSI UNMAP

Una operación SCSI UNMAP requiere aproximadamente un 20 % de espacio libre en el área de almacenamiento de datos de vSphere. Si el área de almacenamiento de datos no cuenta con espacio libre suficiente, su capacidad se llenará durante la operación SCSI UNMAP y, generalmente, una o más máquinas virtuales del área de almacenamiento de datos enviarán a los hosts de vSphere solicitudes de cruce simple de protocolos de datagramas de usuarios a través de traductores de direcciones de red (STUN) hasta que se libere espacio.

Las operaciones SCSI UNMAP implican una gran cantidad de I/O. Realice estas operaciones cuando el arreglo XtremIO no se utilice de manera intensiva, a fin de reducir la probabilidad de que los grupos de usuarios con escritorios alojados en el arreglo experimenten una disminución del rendimiento. Sin embargo, si el arreglo tiene una capacidad física baja, realice la operación SCSI UNMAP inmediatamente, sin importar la carga de I/O actual.

Uso de un script para ejecutar las operaciones SCSI UNMAP

Para recuperar espacio de bloques de almacenamiento sin uso mediante el comando esxcli, ejecute el comando desde un host vSphere conectado al área de almacenamiento de datos de destino. Es posible ejecutar el comando desde una sesión de protocolo SSH al host de vSphere o a través de una sesión de vSphere Management Assistant (vMA) que se conecte al host.

Escriba el siguiente comando, donde *vSphereDatastoreName* corresponde al nombre del área de almacenamiento de datos a la que desea realizar la operación SCSI UNMAP:

```
esxcli storage vmfs unmap -l vSphereDatastoreName -n 20000
```

El comando no muestra ningún resultado y el panel **Recent Tasks en vSphere Web Client no muestra información del estado del comando**. Sin embargo, puede ver el historial de ancho de banda en XtremIO Storage Management Application o en la interfaz de EMC Storage Analytics (ESA) para verificar que la operación finalizó. Para esto, siga los pasos a continuación:

- En XtremIO Storage Management Application, seleccione **Dashboard** › **Performance** › **Bandwidth**.
- En la interfaz de ESA, seleccione **Storage Metrics** › **Metric Picker** › **Total Bandwidth**.

Como se muestra en la Figura 19 y en la Figura 20, es posible identificar fácilmente el impacto de la operación SCSI UNMAP a través del aumento considerable del ancho de banda mientras se ejecuta el comando.

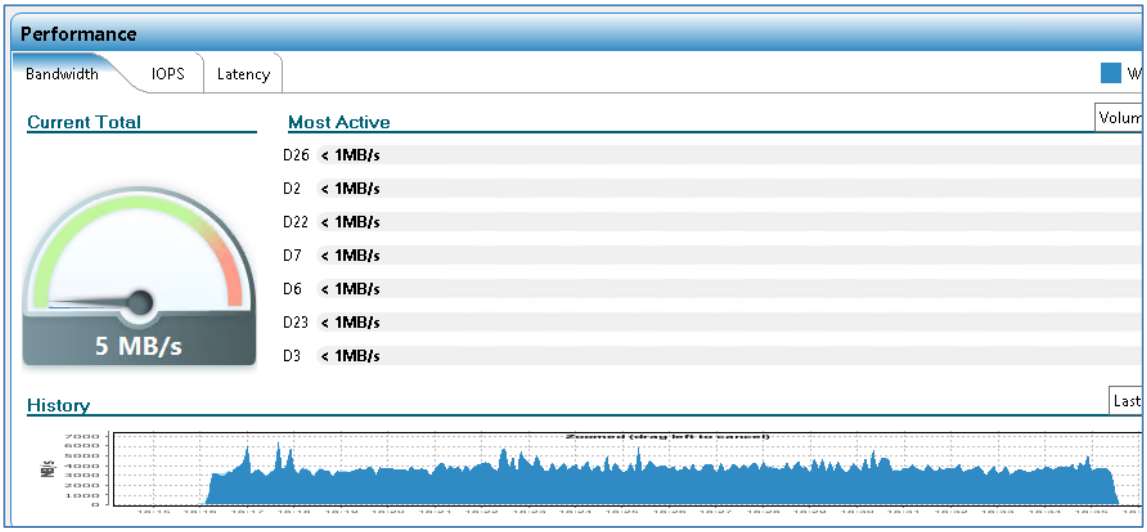


Figura 19. XtremIO Storage Management Application: gráfico de ancho de banda de rendimiento

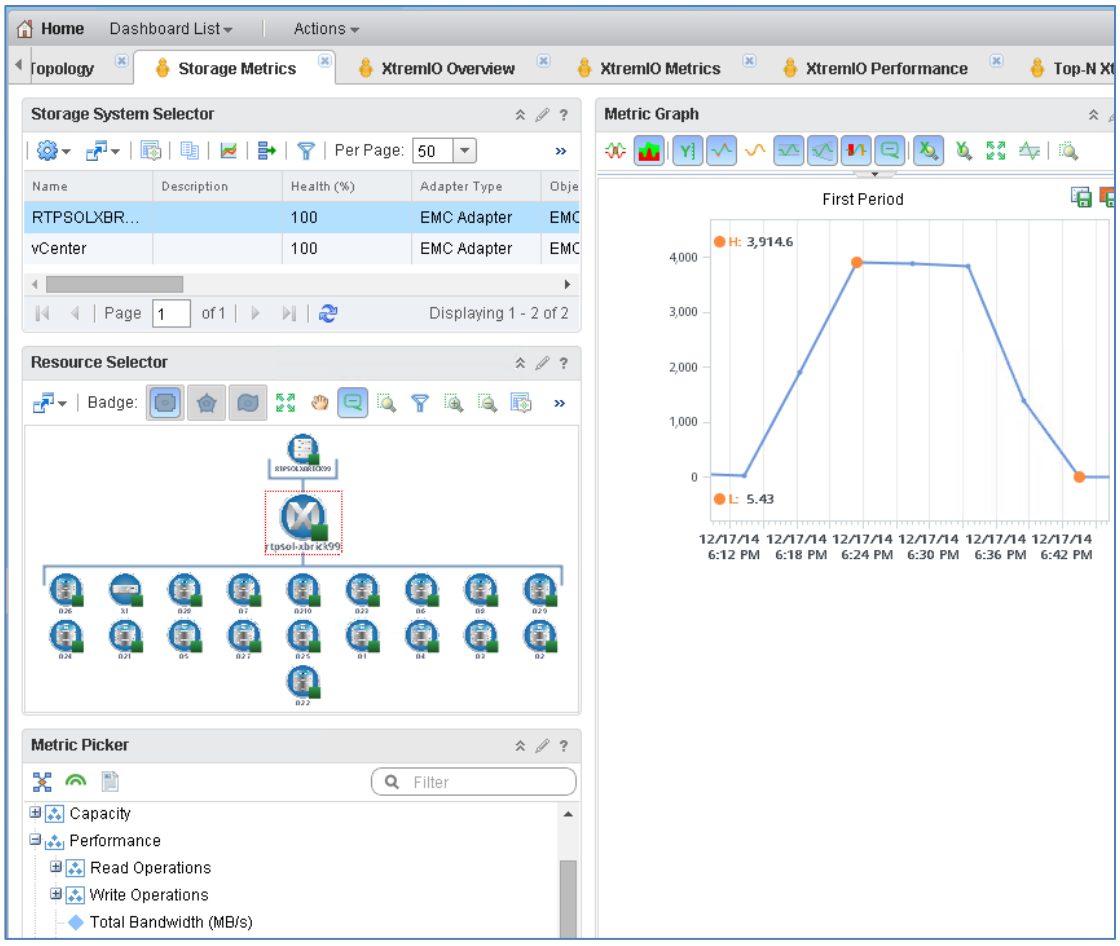


Figura 20. EMC Storage Analytics: gráfico de las métricas de almacenamiento

Uso de EMC VSI para ejecutar las operaciones SCSI UNMAP

Si su solución usa el plug-in de EMC VSI, es posible ejecutar una operación SCSI UNMAP rápidamente desde vSphere Web Client siguiendo los pasos a continuación:

1. En la página de inicio de vSphere Web Client, haga clic en el ícono **Storage**.
2. Haga clic con el botón secundario en el área de almacenamiento de datos de XtremIO de destino para la operación SCSI UNMAP y seleccione **All EMC VSI Plugin Actions** › **Reclaim Unused Storage**, como se muestra en la Figura 21.

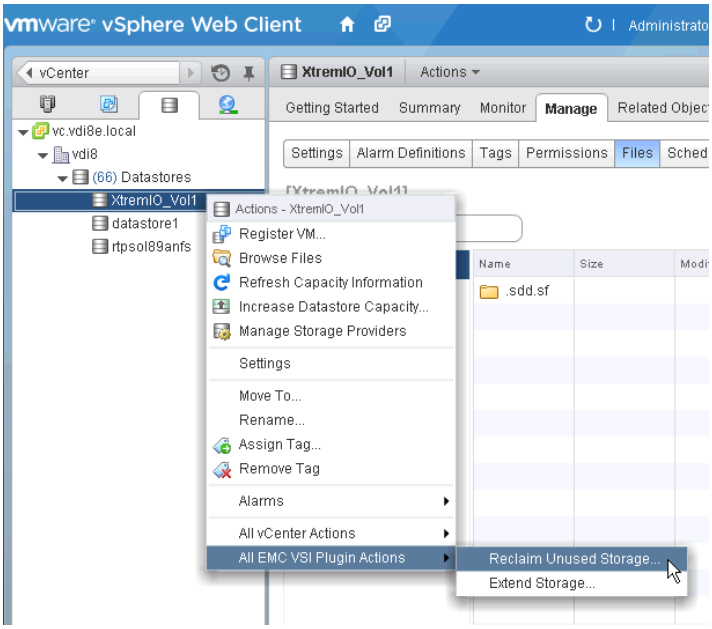


Figura 21. vSphere Web Client: recuperación de espacio de almacenamiento no utilizado en EMC VSI

3. En **Reclamation Details**, escriba el nombre de usuario y la contraseña para una cuenta local en el host de vSphere seleccionado y, a continuación, haga clic en Next.

Nota: La cuenta local debe tener acceso raíz.

EMC VSI seleccionará automáticamente un host para ejecutar la operación SCSI UNMAP, como se muestra en la Figura 22.

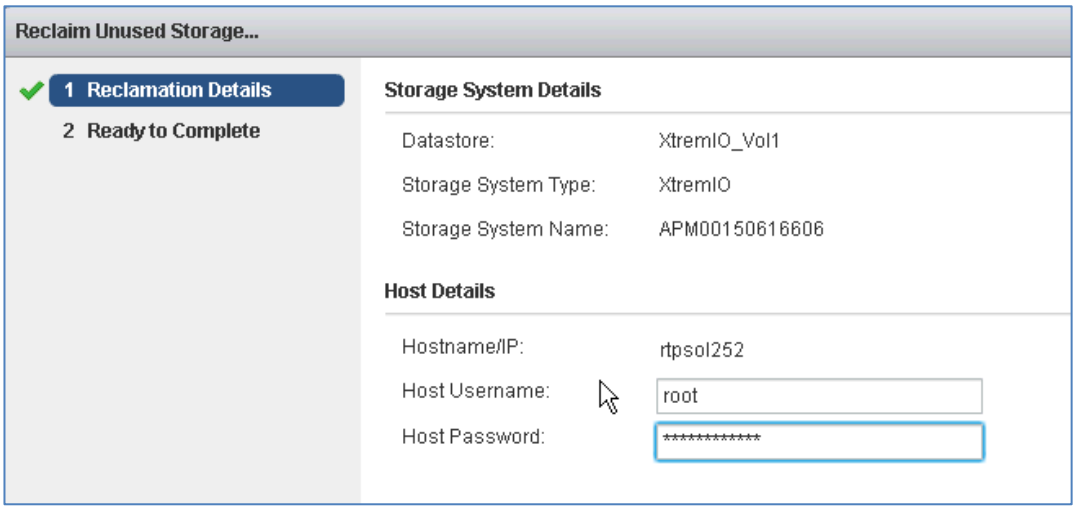


Figura 22. vSphere Web Client: detalles de la recuperación de espacio

4. En **Ready to Complete**, revise los detalles de la operación SCSI UNMAP y, a continuación, haga clic en **Finish**.
5. Seleccione **Recent Tasks › Running** para ver el estado de la operación SCSI UNMAP, como se muestra en la Figura 23.

   También es posible revisar el estado de la operación mediante las estadísticas de ancho de banda del arreglo XtremIO, como se describe en la sección Uso de un script para ejecutar las operaciones SCSI UNMAP.

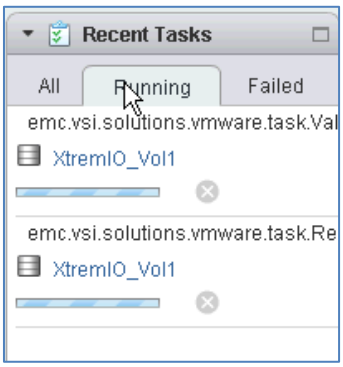


Figura 23. vSphere Web Client: visualización de la pestaña Running en Recent Tasks

Configurar el respaldo y la recuperación de EMC Avamar

Si su solución incluye el respaldo y la recuperación de Avamar, consulte *EMC Backup and Recovery for VSPEX End User Computing for VMware Horizon View: guía de diseño e implementación* para obtener información detallada sobre cómo implementar la solución de respaldo y recuperación.

Configurar VMware vShield Endpoint

En esta sección se proporciona información sobre cómo instalar y configurar los componentes de VMware vShield Endpoint. En la Tabla 17 se describen las tareas que se deben realizar.

Nota: EMC recomienda poner el volumen del SO para vShield Endpoint en el pool de VSPEX Private Cloud. Consulte *VMware vShield Quick Start Guide* para conocer la configuración recomendada de CPU y de memoria.

Tabla 17. Tareas requeridas para instalar y configurar vShield Endpoint

Tarea	Descripción	Referencia
Verificar la instalación del controlador de vShield Endpoint en los escritorios	Verifique que el componente del controlador de vShield Endpoint de las herramientas de VMware se haya instalado en la imagen maestra del escritorio virtual.	*VMware vShield Quick Start Guide*
Implementar el dispositivo vShield Manager	Implemente y configure el dispositivo de vShield Manager.	

Tarea	Descripción	Referencia
Registrar el plug-in de vShield Manager	Registre el plug-in de vShield Manager en el cliente vSphere.	
Aplicar licencias de vShield Endpoint	Aplique los números de licencia de vShield Endpoint con la utilería de licencias de vCenter.	
Instalar el servicio vShield Endpoint	Instale el servicio vShield Endpoint en los hosts vSphere de los escritorios.	
Implementar un servidor de administración de la solución antivirus	Implemente y configure un servidor de administración de la solución antivirus.	*VMware vShield Quick Start Guide* **Nota**: Los partners de vShield Endpoint proporcionan el software del servidor de administración antivirus y las máquinas virtuales de seguridad. Consulte la documentación del proveedor para obtener detalles específicos relacionados con la instalación y la configuración.
Implementar máquinas virtuales de seguridad de vSphere	Implemente y configure máquinas virtuales de seguridad (SVM) en cada host vSphere de los escritorios.	
Verificar la funcionalidad de vShield Endpoint	Verifique la funcionalidad de los componentes de vShield Endpoint utilizando la imagen maestra del escritorio virtual.	**Nota**: Consulte la documentación del proveedor para obtener detalles específicos sobre cómo verificar la integración y la funcionalidad de vShield Endpoint.

Verificar la instalación del controlador de vShield Endpoint en los escritorios

El controlador de vShield Endpoint es un subcomponente del paquete de software de las herramientas de VMware que se instala en la imagen maestra del escritorio virtual. Instale el controlador mediante uno de los siguientes métodos:

- Seleccione la opción **Complete** durante la instalación de las herramientas de VMware.
- Seleccione la opción **Custom** durante la instalación de las herramientas de VMware. En el cuadro de lista VMware **Device Drivers**, seleccione **VMCI Driver** y elija **vShield Driver**.

Para instalar el controlador de vShield Endpoint en una máquina virtual que tenga instaladas las herramientas de VMware, inicie la instalación de las herramientas de VMware y seleccione la opción apropiada.

Implementar el dispositivo vShield Manager

VMware proporciona el dispositivo de vShield Manager como un archivo OVA que se importa a través del cliente de vShield mediante la opción **File › Deploy OVF template**. El dispositivo de vShield Manager está preconfigurado con todos los componentes requeridos.

Instalar el servicio vShield Endpoint

El servicio vShield Endpoint se debe instalar en todos los hosts de escritorios virtuales de vSphere. El dispositivo de vShield Manager instala el servicio en los hosts vSphere. Use la consola web de vShield Manager para iniciar la instalación del servicio vShield Endpoint y para verificar que se realice correctamente.

Implementar un servidor de administración de la solución antivirus

El servidor de administración de la solución antivirus se utiliza para administrar la solución antivirus y es proporcionado por los partners de vShield Endpoint. El servidor de administración y los componentes asociados son un componente requerido de la plataforma vShield Endpoint.

Implementar máquinas virtuales de seguridad de vSphere

Las máquinas virtuales de seguridad de vSphere (SVM) son proporcionadas por los partners de vShield Endpoint y se instalan en cada host de escritorio virtual de vSphere. Las SVM realizan operaciones relacionadas con la seguridad para todos los escritorios virtuales que residen en el host vSphere. Las SVM y los componentes asociados son componentes requeridos de la plataforma vShield Endpoint.

Verificar la funcionalidad de vShield Endpoint

Una vez instalados y configurados todos los componentes requeridos de la plataforma vShield Endpoint, verifique la funcionalidad de la plataforma antes de implementar escritorios virtuales.

Utilizando la documentación proporcionada por el partner de vShield Endpoint, verifique la funcionalidad de la plataforma vShield Endpoint con la imagen maestra del escritorio virtual.

Configurar VMware Workspace

En esta sección se proporciona información sobre cómo instalar y configurar VMware Workspace para la solución. Para realizar una instalación nueva de Workspace, VMware recomienda realizar las tareas en el orden que se muestra en la Tabla 18.

Además de las referencias incluidas en esta sección, la documentación sobre VMware Workspace contiene información adicional necesaria para completar la instalación y la configuración de VMware Workspace.

Nota: EMC recomienda instalar la vApp de VMware Workspace en el pool de nube privada de VSPEX.

Tabla 18. Tareas para la configuración de VMware Workspace

Tarea	Descripción	Referencia
Crear un nuevo pool de IP de vCenter	Cree el pool de IP que VMware Workspace usará para asignar direcciones IP a los dispositivos durante la configuración inicial.	Crear un nuevo pool de IP de vCenter
Asignar direcciones IP y crear registros DNS	Asigne las cuatro direcciones IP necesarias para configurar los dispositivos virtuales de VMware Workspace. Las direcciones IP deben ser diferentes de las utilizadas en el pool de IP.	Asignar direcciones IP y crear registros DNS
Otorgar permisos de retransmisión SMTP de dispositivos de data-va de VMware Workspace	Otorgue los permisos de retransmisión SMTP de dispositivos para que pueda enviar mensajes SMTP relativos a las alertas e información de cuentas de usuario.	• Otorgar permisos de retransmisión SMTP de VMware Workspace • Documentación de servidor de correo electrónico

Tarea	Descripción	Referencia
Configurar una base de datos de PostgreSQL u Oracle para VMware Workspace	Configure una base de datos para que VMware Workspace la use para almacenar información de configuración importante. Se recomienda una base de datos externa por motivos de rendimiento y de escalamiento.	Configurar una base de datos de PostgreSQL u Oracle para
Configurar un recurso compartido CIFS para usar como catálogo de VMware ThinApp (opcional)	De manera opcional, configure un recurso compartido de archivos con permisos de solo lectura para VMware Workspace a fin de activar la distribución de aplicaciones empaquetadas en ThinApp.	• Configurar un recurso compartido CIFS para usar como catálogo de ThinApp (opcional) • *Guía de instalación de EMC VNX5400 Unified* • *Guía de instalación de EMC VNX5600 Unified* • *Guía de introducción del sistema EMC Unisphere*
Verificar que todos los usuarios de VMware Workspace tengan una dirección de correo electrónico especificada	Verifique que todos los usuarios de VMware Workspace tengan direcciones de correo electrónico especificadas.	Verificar que todos los usuarios de VMware Workspace tengan una dirección de correo electrónico especificada
Implementar la vApp de VMware Workspace en vCenter	Implemente la vApp de VMware Workspace, que se proporciona como un archivo OVA que contiene los archivos necesarios para implementar los dispositivos de VMware Workspace.	Implementar la vApp de VMware Workspace en vCenter
Ajustar las especificaciones de la máquina virtual de VMware Workspace (para ambientes que alojan más de 1,000 clientes)	Para ambientes de más de 1,000 usuarios, proporcione recursos adicionales de RAM y CPU a las máquinas virtuales service-va, data-va y gateway-va de VMware Workspace.	Ajustar las especificaciones de la máquina virtual de VMware Workspace
Crear una cuenta de Active Directory que se utilizará para la integración de VMware Workspace en Active Directory	Cree una cuenta de Active Directory para que VMware Workspace pueda sincronizar los datos de las cuentas. La cuenta debe ubicarse dentro de la unidad organizacional (OU) de Active Directory que contiene los usuarios de VMware Workspace de destino.	Documentación del proveedor
Obtener la información requerida para permitir la integración de VMware Workspace en Active Directory	Obtenga la información de la configuración de Active Directory necesaria para permitir que VMware Workspace acceda a Active Directory.	Obtener la información requerida para permitir la integración de VMware Workspace en Active Directory

Tarea	Descripción	Referencia
Crear una cuenta de Active Directory para la integración de VMware Workspace en vCenter Server	Cree una cuenta de Active Directory que se utilizará para la integración de VMware Workspace en vCenter Server.	Documentación del proveedor
Obtener la información de vCenter requerida para permitir la integración de VMware Workspace en vCenter.	Obtenga la siguiente información necesaria para permitir la integración de VMware Workspace en vCenter: • Nombre de host (FQDN) de vCenter • Número de puesto de vCenter • Nombre de usuario para la cuenta de integración de VMware Workspace a vCenter creada previamente • Contraseña para la cuenta de integración de VMware Workspace a vCenter creada previamente	Documentación de VMware Workspace
Obtener el número de licencia de VMware Workspace	Obtenga de VMware el número de licencia de VMware Workspace que activa la plataforma VMware Workspace.	
Tener acceso a la consola del dispositivo configurator-va de VMware Workspace en vCenter	Complete los pasos en el asistente de instalación en el dispositivo configurator-va.	
Utilizar el portal web del configurador de VMware Workspace para completar la configuración de la UI web	Obtenga acceso al portal web del configurador de VMware Workspace en *https://configurator-va-FQDN.*	
Obtener un certificado SSL de confianza y la clave privada para las máquinas virtuales de VMware Workspace (opcional)	Reemplace el certificado SSL con firma propia que VMware Workspace instaló de manera predeterminada. Ni los clientes web ni las máquinas que ejecuten el cliente de software de Workspace confiarán en el certificado.	Obtener un certificado SSL de confianza y la clave privada para las máquinas virtuales de VMware Workspace (opcional)
Activar la autenticación de RSA SecurID (opcional)	De manera opcional, active la autenticación de RSA SecurID a través del portal web del configurador de VMware Workspace en *https://configurator-va-FQDN.*	Documentación de RSA

Tarea	Descripción	Referencia
Configurar el acceso externo al dispositivo de gateway-va de VMware Workspace (opcional)	De manera opcional, active el acceso externo al dispositivo de gateway-va de VMware Workspace.	• Configurar el acceso externo al gateway de VMware Workspace (opcional) • Documentación del proveedor de firewall
Activar la integración de Horizon View (opcional)	De manera opcional, active la integración de Horizon View para permitir a los usuarios acceder a sus escritorios de Horizon View directamente desde el portal de VMware Workspace.	Activar la integración de Horizon View (opcional)
Activar los paquetes ThinApp (opcional)	De manera opcional, active los paquetes ThinApp a fin de que las aplicaciones empaquetadas que utilizan ThinApp se puedan distribuir automáticamente a los clientes que ejecutan el agente de VMware Workspace o se puedan transmitir a los clientes web según demanda.	• *ThinApp User Guide* • *ThinApp Package.ini Parameters Reference Guide*
Activar aplicaciones publicadas por Citrix (opcional)	De manera opcional, active las aplicaciones publicadas por Citrix, lo que permite la integración de VMware Workspace en Citrix XenApp y proporciona acceso a las aplicaciones alojadas por esa plataforma.	Documentación de Citrix XenApp
Brindar a los usuarios el derecho de usar las funciones de VMware Workspace	Use el tablero de VMware Workspace para crear políticas y otorgar acceso a las funciones de VMware Workspace a usuarios y grupos de Active Directory. De forma predeterminada, los usuarios de VMware Workspace no tienen permiso para utilizar ninguna de las funciones de VMware Workspace.	Documentación de VMware Workspace
Capture aplicaciones mediante ThinApp (opcional)	De manera opcional, capture las aplicaciones que usan ThinApp y cárguelas al repositorio de ThinApp de VMware Workspace para que estén disponibles para los clientes que utilizan políticas de VMware Workspace.	• *ThinApp User Guide* • *ThinApp Package.ini Parameters Reference Guide*

Crear un nuevo pool de IP de vCenter

Debe configurar un pool de IP de vCenter con cuatro direcciones disponibles para completar la configuración inicial de la vApp de VMware Workspace. Este pool debe usar direcciones IP en la subred TCP-IP de destino para VMware Workspace y se debe configurar con los valores del dominio DNS y del servidor DNS correctos.

Asignar direcciones IP y crear registros DNS

Durante la implementación, VMware Workspace configura los dispositivos con direcciones IP obtenidas mediante una búsqueda DNS. Cree los registros de DNS para cada una de las cuatro vApps de VMware Workspace antes de implementar las vApp mediante la dirección IP adecuada para cada una. Cree los registros de avance (A) e inversos (PTR).

Otorgar permisos de retransmisión SMTP de VMware Workspace

El dispositivo data-va de VMware Workspace requiere la capacidad de retransmitir mensajes con un servidor SMTP. Configure una dirección de correo electrónico existente para este propósito y verifique que el dispositivo data-va tenga los permisos necesarios.

Configurar una base de datos de PostgreSQL u Oracle para VMware Workspace

Durante la configuración inicial de VMware Workspace, se le solicitará usar la base de datos incorporada predeterminada de PostgreSQL, o bien, una base de datos alojada en un servidor exclusivo que ejecute una versión compatible de Oracle o PostgreSQL. EMC recomienda utilizar un servidor exclusivo para alojar la base de datos de VMware Workspace por motivos de rendimiento y de administración. Debe crear la base de datos antes de la configuración de VMware Workspace siguiendo las instrucciones en *VMware Horizon View Installation Guide*, en el sitio web de VMware.

Configurar un recurso compartido CIFS para usar como catálogo de ThinApp (opcional)

Si utiliza VMware Workspace para ofrecer aplicaciones empaquetadas con VMware ThinApp, cree un recurso compartido de archivo CIFS o Windows para el almacenamiento de aplicaciones. Los requisitos de espacio varían según el número de paquetes que aloje el recurso compartido.

Si utiliza VNX para alojar el recurso compartido, cree el sistema de archivos necesario dentro del pool de almacenamiento del servidor de infraestructura y, a continuación, cree un recurso compartido CIFS. Los usuarios de VMware Workspace requieren acceso de solo lectura a este recurso compartido, mientras que los administradores de ThinApp requieren acceso de lectura y escritura para mantener los paquetes de ThinApp.

Verificar que todos los usuarios de VMware Workspace tengan una dirección de correo electrónico especificada

VMware Workspace requiere que todos los usuarios tengan una dirección de correo electrónico especificada en la cuenta de Active Directory. Si el campo de dirección de correo electrónico de Active Directory está en blanco, significa que los usuarios no están habilitados para VMware Workspace.

La cuenta de Active Directory no necesita estar habilitada para correo electrónico, lo cual es un término utilizado para las organizaciones que utilizan Microsoft Exchange. Solo VMware Workspace requiere que el campo de dirección de correo electrónico de Active Directory del usuario contenga una dirección de correo electrónico válida.

Implementar la vApp de VMware Workspace en vCenter

Si está usando la función Deploy OVF Template en la consola de vCenter, implemente la vApp de VMware Workspace. Para hacerlo, configure los valores de campos siguientes:

- **Host/Cluster**: Cluster de vSphere de nube privada de VSPEX
- **Resource Pool**: Cluster de vSphere de nube privada de VSPEX
- **Storage**: Área de almacenamiento de datos de nube privada de VSPEX
- **Disk Format**: Aprovisionamiento delgado
- **Network Mapping**: Red de destino para las máquinas virtuales de Workspace
- **IP Address Allocation**: Solucionado

Si el ambiente de VMware Workspace es compatible con más de 1,000 usuarios, se deben ajustar las especificaciones de las máquinas virtuales service-va, data-va y gateway-va antes de encender la vApp. Consulte la sección Ajustar las especificaciones de la máquina virtual de VMware Workspace para obtener información sobre cómo realizar estos cambios.

Ajustar las especificaciones de la máquina virtual de VMware Workspace

En la Tabla 19 se detallan los requisitos de recursos de hardware mínimos para ambientes de VMware Workspace que son compatibles con más de 1,000 usuarios. Estos requisitos también se aplican a cualquier máquina virtual data-va adicional que se implemente.

Tabla 19. VMware Workspace para más de 1,000 usuarios: requisitos de recursos de hardware mínimos

vApp	vCPU	Memoria (GB)	Espacio en disco (GB)
Configurator-va	1	1	5
Service-va	6	8	36
Connector-va	2	4	12
Data-va	6	32	175
Gateway-va	6	32	9

Obtener la información requerida para permitir la integración de VMware Workspace en Active Directory

VMware Workspace requiere que las cuentas de usuario de Active Directory se encuentren en una OU distinta de la OU para usuarios predeterminados. Obtenga la siguiente información para esta integración:

- Nombre del controlador de dominio de Active Directory y FQDN
- Contexto de Active Directory para lograr la vinculación, es decir, la raíz de la OU de Active Directory que contiene usuarios y grupos de VMware Workspace, por ejemplo:

  OU=HorizonWorkspace,DC=rtp,DC=lab,DC=emc,DC=com
- DN de Active Directory base de la cuenta de integración de VMware Workspace a Active Directory creada previamente, por ejemplo:

  CN=svc-horizon,OU=HorizonWorkspace,DC=rtp,DC=lab,DC=emc,DC=com
- Contraseña para la cuenta de integración de VMware Workspace a Active Directory creada previamente
- Nombre de usuario y contraseña de Active Directory de una cuenta con el permiso de conectar los equipos al dominio

Obtener un certificado SSL de confianza y la clave privada para las máquinas virtuales de VMware Workspace (opcional)

Puede usar un certificado SSL de confianza y una clave privada asociada para reemplazar el certificado SSL predeterminado y con firma propia de la vApp de VMware Workspace. Si este certificado no se reemplaza, los clientes podrían encontrar errores de validación de SSL al acceder al ambiente de VMware Workspace. Los certificados de raíz e intermedios también son necesarios para completar el proceso de reemplazo del certificado.

Puede usar un solo certificado comodín o reemplazar certificados individuales en cada máquina virtual de VMware Workspace. Los certificados deben estar en el formato PEM.

Configurar el acceso externo al gateway de VMware Workspace (opcional)

Se debe poder acceder a VMware Workspace a través de Internet para usar VMware Workspace como máquina virtual gateway-va para tener acceso externo a Horizon View.

Si se requiere esta funcionalidad, configure el acceso externo como se describe en *Installing and Configuring VMware Workspace Portal* en el sitio web de VMware.

Activar la integración de Horizon View (opcional)

Si VMware Workspace se utiliza como gateway para acceso externo a Horizon View, debe permitir la integración de Horizon View por medio del portal web del configurador en *https://configurator-va-FQDN*.

Configurar VMware vRealize Operations Manager for Horizon View

En esta sección se proporciona información sobre cómo instalar y configurar VMware vRealize Operations Manager for Horizon View. En la Tabla 20 se describen las tareas necesarias.

Nota: EMC recomienda poner el volumen del SO del servidor de vRealize Operations Manager for Horizon View en el pool de VSPEX Private Cloud. Consulte la documentación de vRealize Operations Manager para conocer la configuración de CPU y de memoria recomendada.

Tabla 20. Tareas requeridas para instalar y configurar vRealize Operations Manager

Tarea	Descripción	Referencia
Crear un pool de IP de vSphere para vRealize Operations Manager	Cree un pool de IP con dos IP disponibles para que lo usen las máquinas virtuales de analítica e interfaz del usuario de vRealize Operations Manager.	• *VMware vRealize Operations Manager for Horizon View Installation and Configuration Guide* • *VMware vRealize Operations Manager for Horizon View Administration Guide* • *VMware vRealize Operations Manager for Horizon View Security Guide*
Implementar vSphere Application Services (vApp) de vRealize Operations Manager	Implemente y configure la vApp de vRealize Operations Manager. Ajuste las especificaciones de los dos servidores virtuales que comprenden la vApp de vRealize Operations Manager en función de la cantidad de máquinas virtuales que se monitorean.	

Tarea	Descripción	Referencia
Especificar el vCenter Server que se monitoreará	En la interfaz web principal de vRealize Operations Manager, especifique el nombre del vCenter Server que administra los escritorios virtuales.	
Asignar la licencia de vRealize Operations Manager	Aplique los números de licencia de vRealize Operations Manager for Horizon View mediante la utilería de licencias de vCenter.	
Establecer la configuración de SNMP y SMTP (opcional)	De manera opcional, en la interfaz web principal de vRealize Operations Manager, establezca la configuración de cualquier SNMP o SMTP requerido con fines de monitoreo.	
Actualizar la configuración de escritorios virtuales.	Actualice las políticas y los servicios de firewall de los escritorios virtuales para que sean compatibles con la recopilación de métricas específicas de los escritorios de vRealize Operations Manager for Horizon View.	
Crear la máquina virtual para el servidor del adaptador de vRealize Operations Manager for Horizon View	Cree una máquina virtual en vSphere Client para utilizarla como el servidor del adaptador de vRealize Operations Manager for Horizon View.	
Instalar el SO huésped para el servidor del adaptador de vRealize Operations Manager for Horizon View	Instale Windows Server 2012 R2 como el SO huésped para el servidor del adaptador de vRealize Operations Manager for Horizon View.	
Instalar el software del adaptador de vRealize Operations Manager for Horizon View	Implemente y configure el software del adaptador de vRealize Operations Manager for Horizon View.	
Importar el archivo PAK de vRealize Operations Manager for Horizon View	Importe el archivo PAK del adaptador de vRealize Operations Manager for Horizon View mediante la interfaz web principal de vRealize Operations Manager.	
Verificar la funcionalidad de vRealize Operations Manager for Horizon View	Verifique la funcionalidad de vRealize Operations Manager for Horizon View mediante la imagen principal del escritorio virtual.	

Capítulo 5 Verificación de la solución

Este capítulo presenta los siguientes temas:

Descripción general **72**

Lista de verificación posterior a la instalación **73**

Implementar y probar una sola máquina virtual **73**

Verificar la redundancia de los componentes de la solución **73**

Descripción general

Después de configurar la solución, realice las tareas que se especifican en la Tabla 21. Estas verifican la configuración y la funcionalidad de aspectos específicos de la solución y garantizan que la configuración sea compatible con los principales requisitos de disponibilidad.

Tabla 21. Tareas para comprobar la instalación

Tarea	Descripción	Referencia
Verificar la instalación	Verifique que existan los puertos virtuales adecuados en cada switch virtual del host vSphere.	*VMware vSphere Networking Guide*
	Verifique que cada host vSphere tenga acceso a las áreas de almacenamiento de datos y VLAN requeridas.	• *VMware vSphere Storage Guide* • *VMware vSphere Networking Guide*
	Verifique que las interfaces de vMotion estén configuradas correctamente en todos los hosts vSphere.	*VMware vSphere Networking Guide*
Implementar y probar una sola máquina virtual	Implemente una sola máquina virtual mediante la interfaz de vSphere utilizando la especificación de personalización.	• *VMware vCenter Server and Host Management Guide* • *VMware vSphere Virtual Machine Management Guide*
Verificar la redundancia de los componentes de la solución	Reinicie cada procesador de almacenamiento, uno a la vez, y asegúrese de que se mantenga la conectividad con las áreas de almacenamiento de datos VMware.	Verificar la redundancia de los componentes de la solución
	Desactive cada uno de los switches redundantes, uno a la vez, y verifique que se mantenga la conectividad del host vSphere, de la máquina virtual y del arreglo de almacenamiento.	Documentación del proveedor
	En un host vSphere que contenga por lo menos una máquina virtual, active el modo de mantenimiento y verifique que la máquina virtual pueda migrarse correctamente a otro host.	*VMware vCenter Server and Host Management Guide*
Provisionar los escritorios virtuales restantes	Provisione escritorios mediante máquinas virtuales completas o clones vinculados de View Composer.	*VMware Horizon View Administration Guide*

Lista de verificación posterior a la instalación

Las siguientes tareas de configuración son importantes para la funcionalidad de la solución. Verifique que las tareas se hayan completado antes de implementar esta solución para su uso en producción. En cada servidor vSphere utilizado como parte de esta solución, verifique lo siguiente:

- Los vSwitches que alojan las VLAN cliente estén configurados con puertos suficientes para aceptar el número máximo de máquinas virtuales que puede alojar un host.
- Todos los grupos de puertos de máquinas virtuales requeridos estén configurados y cada servidor tenga acceso a las áreas de almacenamiento de datos de VMware requeridas.
- Hay una interfaz configurada correctamente para vMotion. Consulte la guía *VMware vSphere Networking Guide* para obtener información detallada.

Para obtener mayor información, consulte la lista de documentos en el Documentación de referencia.

Implementar y probar una sola máquina virtual

Implemente una sola máquina virtual para verificar el funcionamiento de la solución. Asegúrese de que la máquina virtual se haya unido al dominio correspondiente, de que tenga acceso a las redes previstas y de que sea posible iniciar sesión.

Verificar la redundancia de los componentes de la solución

Para asegurarse de que los diversos componentes de la solución cumplan los requisitos de disponibilidad, pruebe escenarios específicos relacionados con el mantenimiento o la falla del hardware, como se describe en esta sección.

XtremIO

Reinicie cada controlador de almacenamiento de XtremIO, uno a la vez, y verifique que se mantenga la conectividad con las áreas de almacenamiento de datos VMFS.

1. Inicie sesión en el controlador de almacenamiento A con la cuenta **xinstall**.
2. Reinicie el controlador por medio de la opción **6** en **Install** en la barra de menú.
3. Durante el ciclo de reinicio, compruebe la presencia de áreas de almacenamiento de datos VMFS en los hosts de vSphere.
4. Con la interfaz de XtremIO Storage Management Application, monitoree la ventana de alertas o **Hardware** para verificar que el controlador de almacenamiento A se conecte.
5. Repita este procedimiento con el controlador de almacenamiento B.

Isilon

Si Isilon se implementó como parte de la solución, reinicie cada nodo de Isilon, uno a la vez, y verifique que se mantengan las conexiones a los sistemas de archivos CIFS:

1. Realice la conexión a un nodo disponible en el cluster con un cable en serie o de red.
2. Ejecute el comando **isi status –q** para determinar la dirección IP del nodo que está apagando.
3. Desde el nodo al que se conectó, ejecute el comando ssh para abrir una conexión de protocolo SSH al nodo que se pretende apagar.
4. Ejecute el comando **shutdown -p now** para apagar el nodo.
5. **Ejecute el comando isi status -q** para verificar que el nodo esté apagado.

   El estado del nodo debe ser **D--R** (apagado, de solo lectura). Observe el nodo ID 3 en el siguiente ejemplo:

   ID |IP Address |DASR| In Out Total| Used / Size | Used / Size

   ---+---------------+----+-----+-----+-----+-----------------+-

   1|10.53.217.201 | OK | 48M| 0| 48M| 19G/ 6.2T(< 1%)|(No SSDs)

   2|10.53.217.202 | OK | 46M| 0| 46M| 23G/ 6.2T(< 1%)|(No SSDs)

   3|10.53.217.203 |D--R| n/a| n/a| n/a| n/a/ n/a(n/a)| n/a/n/a(n/a)
6. Con el nodo apagado, verifique que el acceso a los sistemas de archivos CIFS se mantenga o se haya reestablecido.
7. Encienda el nodo que se apagó en el paso 4 y ejecute nuevamente el paso 5. Verifique que el estado del nodo haya vuelto a ser OK.
8. Repita los pasos dos a siete en los nodos de Isilon restantes en el cluster.

VNX

Si se implementó VNX como parte de la solución, ejecute las siguientes tareas de verificación:

1. Reinicie cada procesador de almacenamiento VNX, uno a la vez, y verifique que se mantenga la conectividad con los sistemas de archivos CIFS.
   a. Inicie sesión en Control Station con privilegios de administrador.
   b. Diríjase a **/nas/sbin**.
   c. Ejecute el siguiente comando para reiniciar el SP A:

      ```
      ./navicli -h spa rebootsp
      ```

   d. Durante el ciclo de reinicio, compruebe la presencia de áreas de almacenamiento de datos en los hosts vSphere.
   e. Una vez completado el ciclo, escriba el siguiente comando para reiniciar el SP B:

      ```
      ./navicli -h spb rebootsp
      ```

2. Ejecute un de cada Data Mover de VNX, uno a la vez, y verifique que se vuelva a establecer la conectividad con los sistemas de archivos CIFS.

   a. Desde el indicador $ de Control Station, escriba el siguiente comando y reemplace *movername* con el nombre del Data Mover:

      ```
      server_cpu movername –reboot
      ```

   b. Para verificar que las funciones de redundancia de red funcionen según lo previsto, desactive cada una de las infraestructuras de conmutación redundante, una a la vez. Mientras cada una de las infraestructuras de conmutación está desactivada, verifique que todos los componentes de la solución mantengan la conectividad entre sí y también con cualquier infraestructura del cliente existente.

   c. Utilice la interfaz de Unisphere para reiniciar el sistema.

Host de vSphere

En un host vSphere que contenga por lo menos una máquina virtual, active el modo de mantenimiento y verifique que la máquina virtual pueda migrar a otro host.

Capítulo 6 Documentación de referencia

Este capítulo presenta los siguientes temas:

Documentación de EMC..... 78

Otra documentación 78

Documentación de EMC

Los siguientes documentos, que se encuentran en mexico.emc.com (visite el sitio web de su país correspondiente) o el servicio de soporte en línea de EMC, ofrecen información adicional y pertinente. El acceso a estos documentos depende de sus credenciales de inicio de sesión. Si no tiene acceso a un documento, póngase en contacto con un representante de EMC.

- *Guía del usuario del arreglo de almacenamiento EMC XtremIO*
- *EMC XtremIO Storage Array Operations Guide*
- *EMC XtremIO Storage Array Software Installation and Upgrade Guide*
- *EMC XtremIO Storage Array Hardware Installation and Upgrade Guide*
- *EMC XtremIO Storage Array Security Configuration Guide*
- *EMC XtremIO Storage Array Pre-Installation Checklist*
- *EMC XtremIO Storage Array Site Preparation Guide*
- *Guía de instalación de EMC VNX5400 Unified*
- *Guía de instalación de EMC VNX5600 Unified*
- *Asistente de instalación de EMC VNX para la hoja de trabajo de File/Unified*
- *EMC VNX FAST Cache: A Detailed Review White Paper*
- *Mejores prácticas unificadas para el rendimiento de EMC VNX: Guía de mejores prácticas aplicadas*
- *EMC VSI para el cliente web de VMware vSphere: guía del producto*
- *Guía de instalación de X400*
- Administración de recursos compartidos de SMB y directorios principales de usuarios en EMC Isilon OneFS 6.5 y versiones posteriores
- *Deploying Microsoft Windows 8 Virtual Desktops Applied Best Practices Guide*
- *Guía de instalación y administración de EMC PowerPath/VE para VMware vSphere*
- *EMC PowerPath Viewer Installation and Administration Guide*
- *Respaldo y recuperación de EMC para VSPEX para el cómputo del usuario final con VMware Horizon View: guía de diseño y guía de implementación*
- *Seguridad del cómputo del usuario final EMC VSPEX con RSA SecurID: VMware Horizon View 5.2 and VMware vSphere 5.1 for up to 2,000 Virtual Desktops Design Guide*

Otra documentación

La siguiente documentación, que se encuentra en el sitio web de VMware, brinda información adicional y pertinente:

- *VMware vSphere Installation and Setup Guide*
- *VMware vSphere Networking Guide*
- *VMware vSphere Resource Management Guide*

- *VMware vSphere Storage Guide*
- *VMware vSphere Virtual Machine Administration Guide*
- *VMware vCenter Server and Host Management Guide*
- *Installing and Administering VMware vSphere Update Manager*
- *Preparing the Update Manager Database*
- *Preparing vCenter Server Databases*
- *Understanding Memory Resource Management in VMware vSphere 5*
- *VMware Horizon View Administration Guide*
- *VMware Horizon View Architecture Planning Guide*
- *VMware Horizon View Installation Guide*
- *VMware Horizon View Integration Guide*
- *VMware Horizon View Profile Migration Guide*
- *VMware Horizon View Security Guide*
- *VMware Horizon View Upgrades Guide*
- *VMware Horizon View 6.0 Release Notes*
- *VMware Horizon View Optimization Guide for Windows 7 and Windows 8 White Paper*
- *Installing and Configuring VMware Workspace Portal*
- *Upgrading VMware Workspace*
- *VMware Workspace Administrator's Guide*
- *VMware Workspace Portal User Guide*
- *VMware vRealize Operations Manager for Horizon View Installation and Configuration Guide for Windows and Linux*
- *VMware vRealize Operations Manager for Horizon View Administration Guide*
- *VMware vRealize Operations Manager for Horizon View Security Guide*
- *VMware vShield Administration Guide*
- *VMware vShield Quick Start Guide*

La siguiente documentación, que se encuentra en el sitio web de Microsoft TechNet, brinda información adicional y pertinente:

- *Instalar e implementar Windows Server 2012 R2*
- *Instalación de SQL Server (SQL Server 2012)*

Apéndice A Hoja de trabajo de configuración

Este apéndice presenta el siguiente tema:

Hoja de trabajo de configuración del cliente 82

Hoja de trabajo de configuración del cliente

Antes de configurar la solución, debe reunir cierta información de configuración específica del cliente, como las direcciones IP, los nombres de host, etc.

Las tablas Tabla 22 a la Tabla 29, que se presentan a continuación, proporcionan una hoja de trabajo completamente en blanco que puede usar para reunir esta información.

Para confirmar la información del cliente, puede establecer una referencia cruzada entre esta hoja de trabajo y la siguiente hoja de trabajo de configuración de EMC VNX: *EMC VNX Installation Assistant for File/Unified Worksheet*.

Tabla 22. Información común del servidor

Nombre del servidor	Propósito	Dirección IP principal
	Controlador de dominio	
	DNS primario	
	DNS secundario	
	DHCP	
	NTP	
	SMTP	
	SNMP	
	Consola de VMware vCenter	
	VMware Horizon View Connection Servers	
	Microsoft SQL Server	
	VMware vShield Manager	
	Servidor de administración de la solución antivirus	
	Servidor del adaptador de vRealize Operations Manager for Horizon View	

Tabla 23. Información del servidor vSphere

Nombre del servidor	Propósito	Dirección IP principal	Direcciones de red privada (almacenamiento)	Dirección IP de VMkernel	Dirección IP de vMotion
	Host vSphere 1				
	Host vSphere 2				
	...				

Tabla 24. Información del arreglo XtremIO

Campo	Valor
Nombre del arreglo	
IP de XMS	
Direcciones IP del controlador de almacenamiento	
Nombres de grupos de iniciadores	
Nombres de áreas de almacenamiento de datos	

Tabla 25. Información del arreglo VNX

Campo	Valor
Nombre del arreglo	
Cuenta de administración	
Dirección IP de administración	
Nombre del pool de almacenamiento	
Nombre del recurso compartido CIFS	

Tabla 26. Información del arreglo Isilon

Campo	Valor
Nombre del arreglo	
Cuenta de administración	
Dirección IP de administración	
Nombre de subred	
Pool de IP de subred	
Nombre de zona de SmartConnect	
Nombre de zona de acceso	
Nombre del recurso compartido CIFS	

Tabla 27. Información de la infraestructura de red

Nombre	Propósito	Dirección IP	Máscara de subred	Gateway predeterminado
	Switch Ethernet 1			
	Switch Ethernet 2			
	...			

Tabla 28. Información de VLAN

Nombre	Propósito de la red	ID de VLAN	Subredes autorizadas
	Red de acceso del cliente		
	Red de almacenamiento		
	Red de administración		

Tabla 29. Cuentas de servicio

Cuenta	Propósito	Contraseña (opcional, asegúrela debidamente)
	Administrador de Windows Server	
Root	Raíz de VMware vSphere	
Root	Cuenta raíz del arreglo XtremIO	
xmsupload	Cuenta xmsupload del arreglo XtremIO	
Técnicas	Cuenta técnica XMCLI del arreglo XtremIO	
Root	Raíz del arreglo VNX	
	Administrador del arreglo	
	Administrador de VMware vCenter	
	Administrador de VMware Horizon View	
	Administrador de Microsoft SQL Server	
	Administrador de VMware vRealize Operations Manager	
	Administrador de VMware vShield Manager	